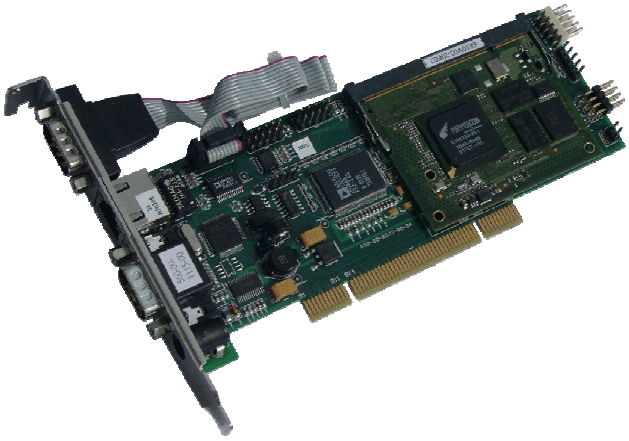
ARMC/3P



User Guide

Release 04.02.00

Copyright © 2007 Acer Inc

Userguide_ARMC/3P_v2
March 2007
100-80-8250-00

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Copyright and Trademark Information

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Acer Inc.

© Copyright 2007 Acer Inc, All rights reserved. Java is a registered trademark of Sun Microsystems, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. The Raritan logo are trademarks of Raritan Computer, Inc. All other marks are the property of their respective owners.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Acer is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Acer modification of the product, or other events outside of Acer's reasonable control or not arising under normal operating conditions.

CE c UL us LISTED 1F61 I.T.E.

For assistance around the world, please see the back cover of this guide for regional Acer Inc contact information.

Downloaded from www.Manualslib.com manuals search engine

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Acer equipment:

- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Downloaded from www.Manualslib.com manuals search engine

Contents

ARMC/3P 1

Contents i

Figures iv

Tables vi

Chapter 1: Introduction 1

Product Overview 1
Product Photos 1
Product Features 3
Terminology 3
Package Contents 5
When the Server is up and running 5
When the Server is dead 6

Chapter 2: Installation 7

Operation Overview 7
Connectors and Jumpers 7
Serial Interface 8
USB Plug 8
Video/USB System Interface 8
10/100 Mpbs Ethernet Adaptor 8
External Power Option 8
Power using ATX Power Cable Adaptor 8
ATX Power Reset 8
Intelligent Management Platform Bus Connector (IPMB) 9
The Set to Default (S2D) Pins 9
Serial 1, Serial 2 and PS/2 9
Placing the ARMC/3P into the Server 11
Open the Server 11
Plugging an ARMC/3P into a PCI Slot 11

Chapter 3: Configuration 17

Initial Configuration 17
ARMC/3P Psetup Tool 17
Using the Psetup Tool via Graphical User Interface 17
Running the Linux Psetup Tool via Command Line 18
Mac Address Detection 20
Authentication 20
Initial Configuration via DHCP Server 21
Initial Configuration via Serial Console 21
Web Interface 22
Mouse, Keyboard and Video configuration 22
ARMC/3P USB interface 22
ARMC/3P Keyboard Settings 23
Remote Mouse Settings 23
Auto Mouse Speed and Mouse Synchronization 23
Host System Mouse Settings 24
Single and Double Mouse Mode 25
Recommended Mouse Settings 25
Video Modes 26
Resetting the ARMC/3P to its Factory Settings 26
Using the S2D Pins 26
Using the Serial Interface 26

Downloaded from www.Manualslib.com manuals search engine

Chapter 4: Usage 27
Prerequisites 27
HTTP/HTTPS 27
Telnet 27
SSH 27
Login into the ARMC/3P and logout 28
Login into the ARMC/3P 28
Navigation 29
Logout from the ARMC/3P 31
Managing the ARMC/3P with a CommandCenter 31
The Remote Console 31
General Description 31
Main Window 32
Remote Console Control Bar 33
Remote Console Options 34
Remote Console Status Line 44
Optimizing the Video Picture 45
Reducing the Noise of the Video Picture 46
Using the ARMC/3P with low bandwidth 47

Chapter 5: Menu Options 49
Remote Control 49
KVM Console 49
Remote Power 49
Telnet Console 51
Virtual Media 54
Floppy Disk 54
CD ROM 55
Drive Redirection 59
Options 62
Creating an Image 63
System Health 65
Chassis Control 65
Monitor Sensors 65
System Event Log 66
Alarm Settings 66
User Management 67
Change Password 67
User and Groups 67
Permissions 69
KVM Settings 70
User Console 70
Power Control 73
Keyboard/Mouse 74
Video 75
Device Settings 78
Network 78
Dynamic DNS 81
Security 83
Certificate 86
Serial Port 89
Intelligent Platform Management Interface (IPMI) 92
Date/Time 93
Authentication 93
Event Log 96
SNMP Settings 98
Maintenance 101
Device Information 101
Language 102
Event Log 103
Update Firmware 103
Unit Reset 104

Appendix A: Specifications 105
Sizes and Weights 105
Environment 105
Temperature 105

Downloaded from www.Manualslib.com manuals search engine

Humidity....105

Appendix B: ARMC/3P Video Modes....107

Appendix C: Key Codes....109

Appendix D: Pin Assignment....111

VGA HD-15....111
RJ45 Connetcor Ethernet....111
IPMB/I2 Connector....111
Serial SUB-D9 Connector 1....112
PS/2 Connector....112
USB....112

Appendix E: Troubleshooting....113

Appendix F: GNU General Public License (GPL)....115

Appendix G: The OpenLADAP Public License....121

Downloaded from www.Manualslib.com manuals search engine

Figures

Figure 1 ARMC/3P with High-Profil Bracket 1
Figure 2 24-pole ATX Power Cable Adaptor 1
Figure 3 ARMC/3P with Low-Profil Bracket 2
Figure 4 IPMB Cable, Power Cable, Reset Cable 2
Figure 5 Serial Cable 2
Figure 6 VGA-USB System Cable and PS/2 System Cable 2
Figure 7 ARMC/3P Internal Connectors 7
Figure 8 Connection of the ARMC/3P VGA-USB System Cable 7
Figure 9 ARMC/3P Reset/Power Connection Pinout 9
Figure 10 ARMC/3P with PS/2 10
Figure 11 PS/2 System Cable 10
Figure 12 Mounting the ARMC/3P into a PCI Slot 11
Figure 13 IPMB Cable 11
Figure 14 IPMB Connector 12
Figure 15 Power using Reset/Power Wires 12
Figure 16 Power using ATX Power Cable Adaptor 14
Figure 17 ARMC/3P Psetup Tool (Windows Version) 18
Figure 18 ARMC/3P Psetup Tool (Linux Version) 18
Figure 19 Remote Console Control Bar: Sync Button 24
Figure 20 Terminal with Reset Message 26
Figure 21 The Internet Explorer displaying the Encryption Key Length 28
Figure 22 Login Screen 28
Figure 23 Password Change Request 29
Figure 24 ARMC/3P Main Page Overview 30
Figure 25 Navigation Frame Overview 30
Figure 26 Logout Link 31
Figure 27 Remote Console 32
Figure 28 Remote Console Control Bar 33
Figure 29 Remote Console Options Menu 34
Figure 30 Remote Console Options Menu: Scaling 35
Figure 31 Remote Console Options Menu: Mouse Handling 36
Figure 32 Remote Console Options Menu: Local Cursor 37
Figure 33 Remote Console Options Menu: Chat Window 37
Figure 34 Remote Console Options Menu: Video Settings Panel 39
Figure 35 Remote Console Options Menu: Softkeyboard 41
Figure 36 Soft Keyboard Mapping 41
Figure 37 Remote Console Options Menu: Hotkey Confirmations Dialog 42
Figure 38 Remote Console Options Menu: Encoding - Predefined 42
Figure 39 Remote Console Options Menu: Encoding - Compression 43
Figure 40 Remote Console Options Menu: Encoding – Color Depth 44
Figure 41 Remote Console Status Line 44
Figure 42 Status Line Transfer Rate 45
Figure 43 Remote Console Video Settings: Reset this Mode 46
Figure 44 Main Page with Remote Console Preview 49
Figure 45 Power Control Overview 50
Figure 46 ‘Internal Power Control’ Buttons 50
Figure 47 ‘Power Control via IPMI’ Buttons 51
Figure 48 Telnet Console 52
Figure 49 Floppy Virtual Area 54
Figure 50 Select Image File 55
Figure 51 Active Image File 55

Downloaded from www.Manualslib.com manuals search engine

Figure 52 Selecting CD-ROM and Windows Share 56
Figure 53 The Image File on the Share 57
Figure 54 Explorer Context Menu 58
Figure 55 Share Configuration Dialog 58
Figure 56 Drive Redirection 59
Figure 57 Main View 60
Figure 58 Selecting the desired Drive 61
Figure 59 Selection Write Support 61
Figure 60 Device Authentification 61
Figure 61 Virtual Drive Selection 62
Figure 62 Tray Info 62
Figure 63 USB Mass Storage Option 62
Figure 64 RawWrite for Windows Selection Dialog 63
Figure 65 Nero Selection Dialog 64
Figure 66 Chassis Control 65
Figure 67 Monitor Sensors Overview 66
Figure 68 System Event Log Overview 66
Figure 69 IPMI Alarm Configuration 66
Figure 70 Set Password 67
Figure 71 User/Group Management 67
Figure 72 User/Group Permission Settings 69
Figure 73 User Console Settings (Part 1) 70
Figure 74 User Console Settings (Part 2) 71
Figure 75 Power Control 73
Figure 76 Keyboard and Mouse Settings 74
Figure 77 Video Settings 77
Figure 78 Network Settings 78
Figure 79 Dynamic DNS 81
Figure 80 Dynamic DNS Scenario 81
Figure 81 Security Settings 83
Figure 82 Certificate Settings 87
Figure 83 SSL Certificate Upload 88
Figure 84 Serial Settings 90
Figure 85 IPMI Settings 92
Figure 86 Date and Time 93
Figure 87 Authentication Settings 95
Figure 88 Event Log Settings 97
Figure 89 SNMP Settings 99
Figure 90 Device Information 101
Figure 91 Connected Users 101
Figure 92 Voltages Overview 102
Figure 93 Language Settings 102
Figure 94 Event Log List 103
Figure 95 Update Firmware Dialog 103
Figure 96 Unit Reset 105
Figure 97 English (US) keyboard Layout, used for the key codes 109
Figure 98 VGA HD-15 111
Figure 99 RJ45 111
Figure 100 Serial Connector 112

Downloaded from www.Manualslib.com manuals search engine

Tables

Table 1 Hardware Failures 6
Table 2 Host System Failures and how they are detected 6
Table 3 Voltage and Power Specification 14
Table 4 Initial Network Configuration 17
Table 5 Serial Line Parameters 21
Table 6 Standard User Settings 22
Table 7 Standard User Settings 29
Table 9 Links for Navigation 30
Table 10 Buttons displaying the Access Status 45
Table 11 Buttons displaying the Monitor State 45
Table 12 ARMC/3P Specifications 105
Table 13 Temperature 105
Table 14 Humidity 105
Table 15 ARMC/3P Video Modes 107
Table 16 Key Names 109
Table 17 VGA HD-15 111
Table 18 RJ45 111
Table 19 IPMB/I2C Connector 111
Table 20 Serial Connector 1 112
Table 21 Serial Connetcor 2 112
Table 22 PS/2 Connector 112
Table 23 USB Connector 112

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Chapter 1: Introduction

Product Overview

The ARMC/3P is a manufacturer-independent remote administration system. The ARMC/3P works as an integrated solution on your server system. Based on an embedded operating system, the ARMC/3P provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, you have entire control and location-independent remote access to react upon both critical incidents and cases of necessary maintenance.

Product Photos

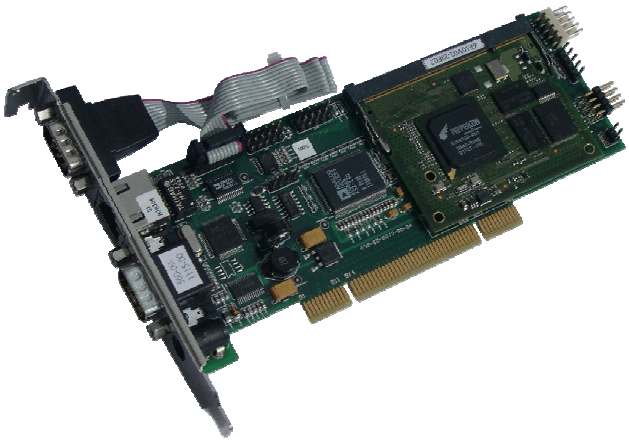


Figure 1 ARMC/3P with High-Profil Bracket

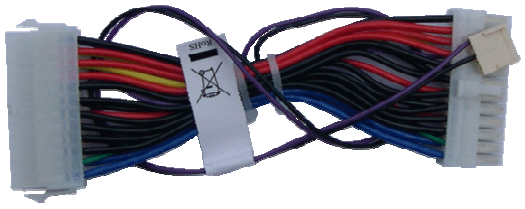


Figure 2 24-pole ATX Power Cable Adaptor

Downloaded from www.Manualslib.com manuals search engine

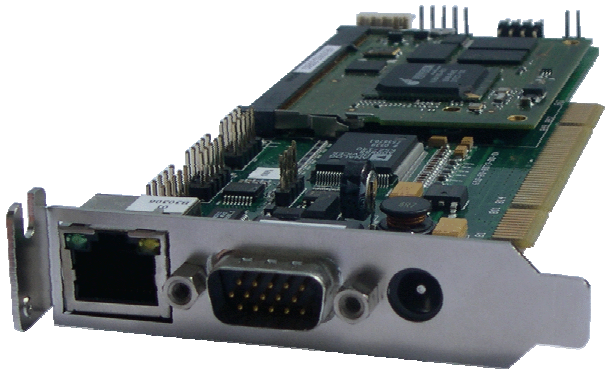


Figure 3 ARMC/3P with Low-Profil Bracket

Figure 4 IPMB Cable, Power Cable, Reset Cable

Figure 5 Serial Cable

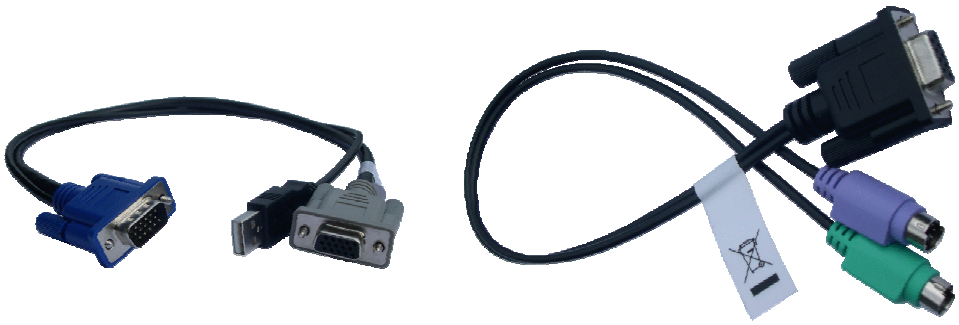


Figure 6 VGA-USB System Cable and PS/2 System Cable

Downloaded from www.Manualslib.com manuals search engine

Product Features

The ARMC/3P defines a new class of remote access devices. It combines digital remote access via IP networks with comprehensive and integrated system management. The ARMC/3P offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs on its embedded processors only, but not on mission critical servers, so there is no interference with server operation or impact on network performance.

Furthermore, the ARMC/3P offers additional remote power management with the help of optional available devices. Features of the ARMC/3P are:

- KVM (keyboard, video, mouse) access over IP or telephone line
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Port to connect a user console for direct analogous access to KVM device
- Local mouse suppression (only when using SUN's Java Virtual Machine)
- Remote Power Management
- Remote Virtual Media

Terminology

ACPI

Advanced Configuration and Power Interface
A specification that enables the operating system to implement power management and system configuration.

ATX

Advanced Technology Extended
A specification that covers the style of motherboards and enclosures introduced by Intel in 1995.

Client

The workstation of the user for connecting the host system through the ARMC/3P.

DHCP

Dynamic Host Configuration Protocol
A protocol for dynamically assigning IP addresses to host names, especially used in a local network.

DNS

Domain Name System
A protocol used to locate computers on the Internet by their name.

FAQ

Frequently Asked Questions

Downloaded from www.Manualslib.com manuals search engine

Host

Host System
The server system which is hosting the ARMC/3P.

HTTP

Hypertext Transfer Protocol
One of the protocols used for communication between single computers, especially between web browsers and web servers.

HTTPS

Hypertext Transfer Protocol Secure
The secure version of HTTP.

IPMI

Intelligent Platform Management Interface
A specification defining a set of common interfaces for operating system independent platform management and health monitoring.

LED

Light Emitting Diode
A semiconductor device that emits incoherent monochromatic light when electrically biased in the forward direction.

PS/2

Personal System/2
IBM's second generation of personal computers, which was released to the public in 1987. Today, PS/2 is known as a device interface for mouse and keyboard.

SNMP

Simple Network Management Protocol
A widely used network monitoring and control protocol.

SSH

Secure Shell
An encrypted network protocol providing a secure replacement for Telnet.

SSL

Secure Socket Layer
An encryption technology for the Internet used to provide secured data transmissions.

SVGA

Super Video Graphics Array
A refinement of the Video Graphics Array (VGA) that provides increased pitch and resolution performance.

UTP

Unshielded Twisted Pair
A cable with two conductors twisted as a pair and bundled within the same outer PVC covering.

Downloaded from www.Manualslib.com manuals search engine

Package Contents

The ARMC/3P comes as a regular PCI card and is shipped with:

- an ARMC/3P Board with High-Profile Bracket
- a VGA-USB System Cable
- an IPMB Cable
- an ATX Reset/Switch Cable
- a Videosplitter cable for Local Console
- a CD ROM with User Manual and utilities
- a Quick Start Guide
- an External Power supply # TZ.30400.006 [1]

1. In EMEA Region the ARMC/3P card is shipped by default with the External Power Adaptor, In order to make the ARMC/3P card System independent. In other regions it is an optional item.

Available separately (optional):

- Power Pack US (PWRPK-US-5mm) # TZ.30400.004
  - External Power Supply
  - AC Power Cord US
- Power Pack UK (PWRPK-UK-5mm) # TZ.30400.005
  - External Power Supply
  - AC Power Cord UK
- Power Pack EU (PWRPK-EU-5mm) # TZ.30400.006
  - External Power Supply
  - AC Power Cord EU

When the Server is up and running

The ARMC/3P gives you full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirection Service you can do the following:

- Reboot the system (a graceful shutdown)
- Watch the boot process
- Boot the system from a separate partition or from Virtual Media to load the diagnostic environment or install operating systems
- Run special diagnostic programs

Downloaded from www.Manualslib.com manuals search engine

When the Server is dead

Obviously, fixing hardware defects is not possible using a remote management device. Nevertheless, the ARMC/3P gives the administrator valuable information about the type of a hardware failure. Serious hardware failures can be categorized into five different categories with different chances to happen [1]:

Table 1 Hardware Failures

Category	Probability
Hard disk failure	50 %
Power cable detached, power supply failure	28 %
CPU, Controller, motherboard failure	10 %
CPU fan failure	8 %
RAM failure	4 %

Using the ARMC/3P, administrators can determine which kind of serious hardware failure has occurred (see Table 2).

Table 2 Host System Failures and how they are detected

Category	Probability
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remeians in power off state after power on command has been given.
CPU, Controller, motherboard failure	Power supply is on, but there is no video putput.
CPU fan failure	By IPMI or server specific management software
RAM failure	Boot-Sequence on boot console

Note: According to a survey made by the Intel Corp.

Downloaded from www.Manualslib.com manuals search engine

Chapter 2: Installation

Operation Overview

The ARMC/3P redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol family.

The ARMC/3P can be used in both a multi-administrator and multi-server environments. Combining one or more ARMC/3P with a single KVM switch allows acess to multiple servers on a single remote console.

Connectors and Jumpers

Figure 7 and Figure 8 show all connectors and plugs of the ARMC/3P. Each of these connectors will be explained in the following.

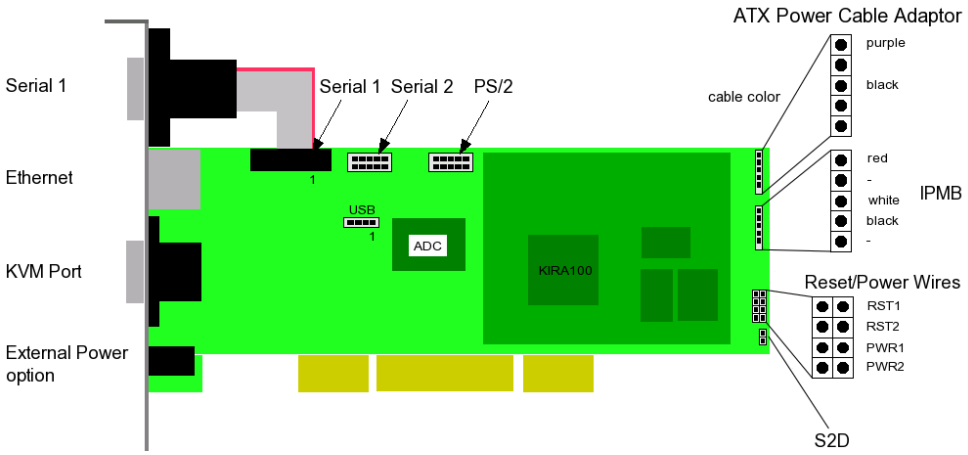


Figure 7 ARMC/3P Internal Connectors

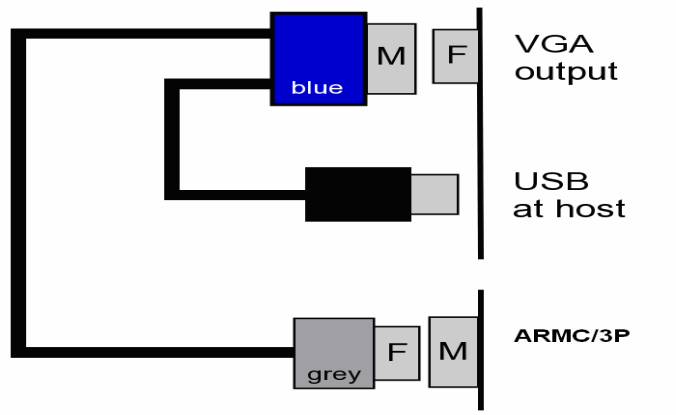


Figure 8 Connection of the ARMC/3P VGA-USB System Cable

Downloaded from www.Manualslib.com manuals search engine

Serial Interface

An optional external modem may be connected to the ARMC/3P using this connector. The connector is compliant to the RS 232 serial line standard with hardware handshake.

Every off-the-shelf modem can be connected to the ARMC/3P via the RS 232 interface. For details on configuring and using the serial interface please see **Chapter 5**: **Serial Port**.

USB Plug

Use this connector to connect the ARMC/3P with the host's USB interface.

Video/USB System Interface

This interface combines both the USB and the Video input connector of the ARMC/3P. Please connect the supplied system cable to the connector, only.

10/100 Mpbs Ethernet Adaptor

UTP Cat 3 or 5 cables can be connected to the ARMC/3P using a standard RJ45 jack. Refer to Appendix F for the details of the pin assignment for the RJ45 connector.

External Power Option

To allow the ARMC/3P to operate independently from the server system, An external power supply must be connected to the ARMC/3P. Please see **Chapter 2: Connecting Optional External Power Supply** for further details.

Power using ATX Power Cable Adaptor

The 20–pole or 24-pole ATX Power Cable Adaptor has to be connected to the ARMC/3P and between the motherboard and the host power supply for the internal powering of the ARMC/3P. Please see **Chapter 2: Connecting Power using ATX Power Cable Adaptor** for further details.

ATX Power Reset

Additional cables are required in order to enable the remote reset and the remote power functions of the ARMC/3P. The reset/power switch has the pin assignment as shown in Figure 9. Please see **Chapter 2: Connecting to ATX Control Signals** for further details.

Downloaded from www.Manualslib.com manuals search engine

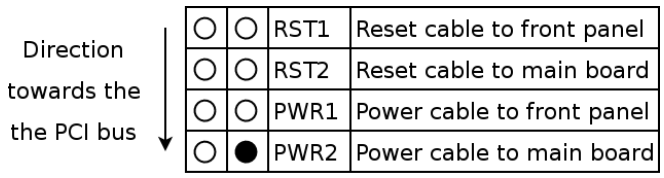


Figure 9 ARMC/3P Reset/Power Connection Pinout

Note: On the ARMC/3P the pin for the power connector is tagged with "ATX".

Intelligent Management Platform Bus Connector (IPMB)

The IPMB connector on an IPMI capable motherboard allows direct access to power control functions. Connecting the IPMB connector of the ARMC/3P with such a port using our IPMB cable makes it possible to use the IPMI over IPMB function of the ARMC/3P. Refer to **Appendix D: Pin Assignment** for the pin assignment details of the IPMB connector.

The Set to Default (S2D) Pins

These pins may be used to reset the ARMC/3P to its factory settings. See **Chapter 3: Resetting the ARMC/3P to its Factory Settings** for a detailed description on how to reset the ARMC/3P.

Serial 1, Serial 2 and PS/2

If your server does not support USB keyboard and/or mouse in all states but only PS/2 mouse and keyboard, you need the PS/2 system cable to connect the ARMC/3P. The proprietary PS/2 to Sub D9 cable enables the control over the host system. The following steps describe how to use this PS/2 system cable.

1. The flat cable from the serial port (Sub D9 connector) of the High-Profile Bracket has to be connected to the PS/2 pins on the ARMC/3P (see Figure 10).
2. Connect the PS/2 cable to the serial port (Sub D9) (see Figure 11 PS/2 System Cable).

Downloaded from www.Manualslib.com manuals search engine

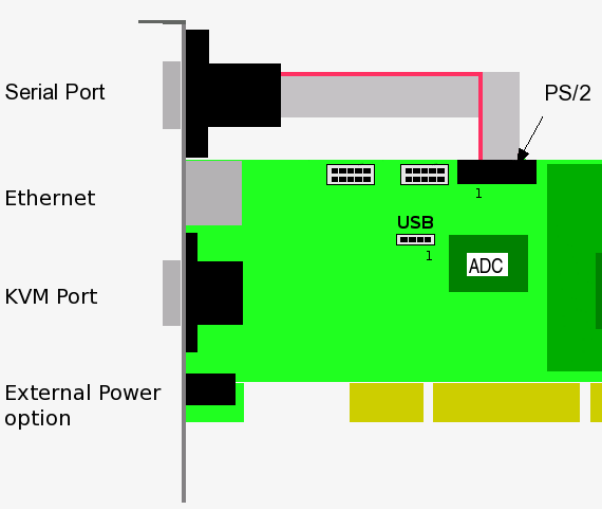


Figure 10 ARMC/3P with PS/2

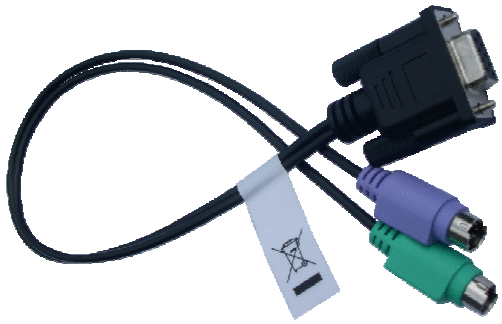


Figure 11 PS/2 System Cable

There are only 9 PS/2 pins on the ARMC/3P. Therfore the PS/2 system cable offers only the connection from ARMC/3P to the server. Connecting local PS/2 mouse and keyboard to the server is no longer possible!

There are the following function restrictions:

- If using the Low-Profile Bracket, then there is no serial or PS/2 connection possible. Except for using additional brackets for offering the missing connection.
- If using the High-Profile Bracket, then you have either the serial connector or the PS/2 connector. Except for using an additional bracket to offer the missing connection.
- If using PS/2 connection from ARMC/3P to server, then the local mouse and keyboard have to be connected via USB.

Downloaded from www.Manualslib.com manuals search engine

Placing the ARMC/3P into the Server

Open the Server

In order to install the ARMC/3P you need to open the host system. Detach the host from its power cable and follow the instructions of your system documentation.

Plugging an ARMC/3P into a PCI Slot

ARMC/3P PCI

Place the ARMC/3P into a free PCI slot. You may use any PCI slot (33 or 66 MHz, 32 or 64 Bit, PCI-X).

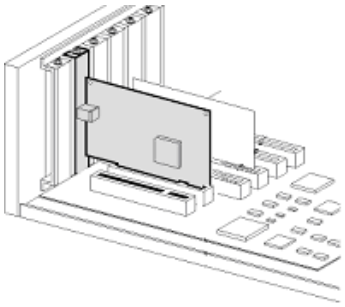


Figure 12 Mounting the ARMC/3P into a PCI Slot

Connecting Power and Reset Cables

The ARMC/3P offers the possibility to remotely control both the power and the reset functions of the host system. In order to support it, there is additional cabling necessary. The preferred way for this cabling are the interfaces offered by IPMI. However, if your host does not support IPMI you may use one of the other possibilities.

Connecting over IPMB

This connection is used to power on or power off the system, or to perform a hard reset. You must have a motherboard that supports IPMI 1.5 or higher and has a 3 or 4 pin IPMB connector as shown in Figure 14

- Connect the 5 pin connector of the IPMB cable with the 1x5 pin IPMB connector on the ARMC/3P as shown in Figure 7.
- Connect the other ending of the cable with one of the IPMB connectors (3 or 4 pin connector) on the motherboard.
- Set the IPMI settings to IPMI over IPMB.
- Make sure that the IPMI function is enabled on the host system.

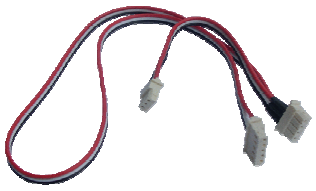


Figure 13 IPMB Cable

Downloaded from www.Manualslib.com manuals search engine

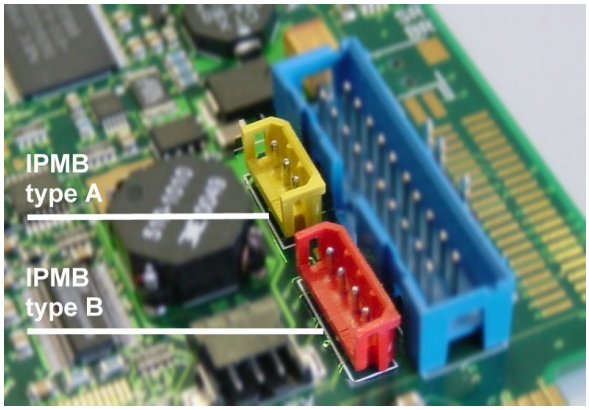


Figure 14 IPMB Connector

Connecting to ATX Control Signals

In case your system provides separated pins for reset and power on/off, perform the following steps while referring to Figure 7 ARMC/3P Internal Connectors.

1. Find the cable connecting the front panel reset button and the motherboard.
2. Disconnect this cable from the motherboard and connect it to RST2 of the ARMC/3P. Refer to Figure 9 for pin assignment.
3. Take the reset cable provided with the ARMC/3P and connect one end to the motherboard's reset connector (from where you just disconnected the cable to the front panel), and the other end to RST1 of the RST/PWR connector of the ARMC/3P.
4. Find the cable connecting the front panel power button and the motherboard.
5. Disconnect this cable from the motherboard and connect it to PWR2. For pin assignment details, refer to Figure 9.
6. Take the power cable provided with the ARMC/3P and connect one end to the motherboard's power connector (from where you just discon- nected the cable to the front panel), and the other end to PWR1 of the RST/PWR connector of the ARMC/3P.
7. Check the cabling: there are four cables connected to the RST/PWR connector, finally.

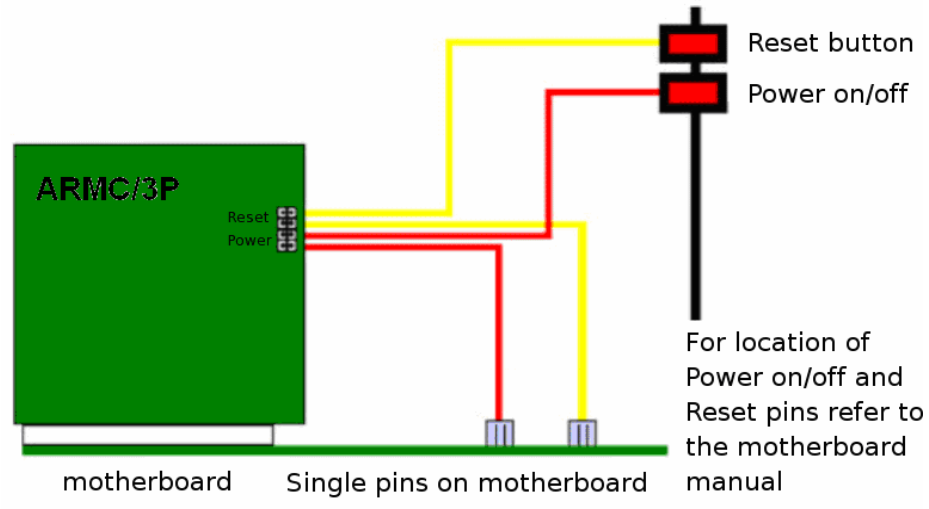


Figure 15 Power using Reset/Power Wires

Downloaded from www.Manualslib.com manuals search engine

Connecting with Front Panel Connector

There are motherboards which do not have separated pins for power on/off and reset. Both the reset and the power buttons are placed on the system's front panel and connected to the motherboard via a common front panel connector. To allow the connection of the ARMC/3P's remote reset and power on/off signals to those motherboards a special front panel adapter has to be placed between the front panel connector on the motherboard and the cable connector to the front panel. Please ask your local service center for assistance.

Connecting Power Supply

The ARMC/3P offers the possibility to be powered internally by the host system using the ATX Power Adaptor cable or powered externally using the external Power adaptor. (see **Package Contents**).

Connecting Power using ATX Power Cable Adaptor

If the host system provides an ATX 20 or ATX 24 (EPS) connection from the power supply to the motherboard, this cable can be extended with the delivered ATX Power Cable Adaptor. In that case the ARMC/3P is powered internally using the 5V Standby Power of the host power supply. There is no other external power supply necessary.

For connecting the ATX Power Cable Adaptor obey the following steps while referring to Figure 7.

1. Power off the host and disconnect it from the power line.
2. Find the ATX cable connecting the host system power supply and the motherboard and remove the cable.
3. Exchange the disconnected cable with the delivered 20-pole ATX Power Cable Adaptor or the 24-pole ATX Power Cable Adaptor (EPS) cable. Then, connect the male connector of the enclosed ATX Power Cable Adaptor to the power supply of the host system and connect the female connector of the enclosed ATX Power Cable Adaptor to the power connector of the motherboard.
4. Connect the ATX Power Cable Adaptor male connector on the ARMC/3P with the 5 pin female connector of the ATX Power Cable Adaptor. Refer to Figure 16 ARMC/3P Host Power pins
5. Check the cabling, finally.

Note: Powering the ARMC/3P using ATX Power Cable Adaptor solution requires Standard ATX Power Supply with 5V/2A Standby Power. Refer to the host system and/or power supply manual if the host system and the host power supply fully support the ATX standard.

Downloaded from www.Manualslib.com manuals search engine

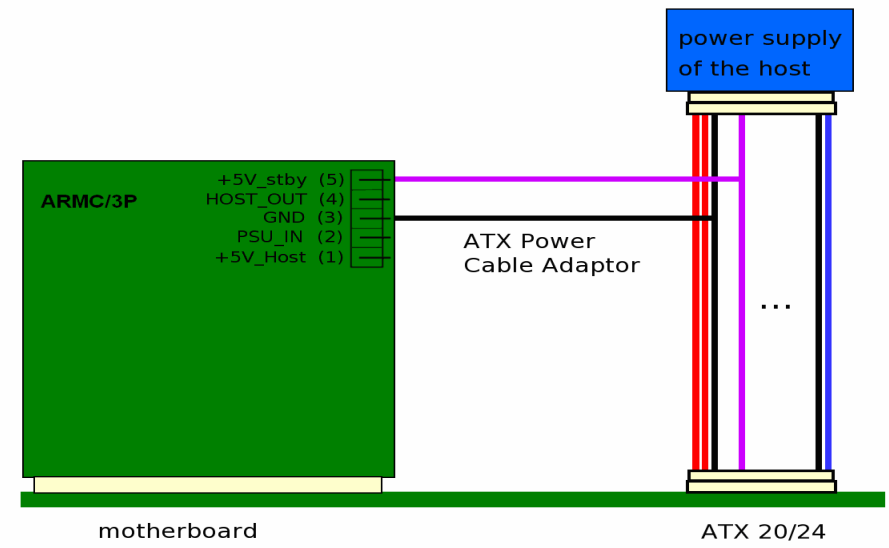


Figure 16 Power using ATX Power Cable Adaptor

Connecting Optional External Power Supply

To allow the ARMC/3P to operate independently from the server system it is possible to connect the card to an external power supply. From the technical point of view any power supply can be used as long as the following specifications are met:

Table 3 Voltage and Power Specification

Parameter	Value
Voltage	5V
Current	>= 1A
Pinning	Plus on inner connector
Dimension	2.1 mm diameter

We recommend a 5V /1A power supply. Contact your local sales representative for an Acer approved power supply.

Important: Any standard power supply compliant with the requirements stated above may be used. Nevertheless, any warranty from Acer voids if non-Acer power supplies are used in conjunction with the ARMC/3P. Check for the Acer approval label on the external power supply in order to preserve your manufacturer's warranty.

Connecting Keyboard and Mouse

Keyboard and mouse data are transmitted via USB into the server system. Connect the USB plug into the appropriate socket on the server. Local USB keyboard and mouse could be plugged into the host directly and parallel to the ARMC/3P VGA-USB cable.

Downloaded from www.Manualslib.com manuals search engine

Connecting Ethernet

The bracket of the ARMC/3P provides a RJ45 connector for Ethernet. The connector is used either for a 100 Mbps 100Base-TX connection or for a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will adjust to the appropriate operation mode automatically.

10 Mbps Connection

For 10BASE-T Ethernet networks the Fast Ethernet adapter uses category 3, 4, or 5 UTP cable. To establish a 10 Mbps connection, the cable has to be connected to a 10BASE-T hub.

1. Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
2. Align the RJ45 plug with the notch on the adapter 's connector and insert it into the adapter 's connector.

100 Mbps Connection

For 100BASE-TX Ethernet networks the ARMC/3P supports category 5 UTP cabling. To establish a 100 Mbps connection, the cable has to be connected to a 100BASE- TX hub.

1. Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
2. Align the RJ45 plug with the notch on the adapter 's connector and insert it into the adapter 's connector.

Important: The UTP wire pairs and configuration for 100 BASE-TX cable are identical to those for 10 BASE-T cable when used with category 5 UTP cable.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Chapter 3: Configuration

Initial Configuration

The ARMC/3P's communication interfaces are all based on TCP/IP. It comes preconfigured with the IP configuration listed in Table 4 Initial Network Configuration.

Table 4 Initial Network Configuration

Parameter	Value
IP auto configuration	DHCP
IP address	none
Netmask	255.255.255.0
Gateway	none
IP access control	none

Important: If the DHCP connection fails on boot up, the ARMC/3P will not have an IP adresss.

If this initial configuration does not meet your requirements, the following describes the initial IP configuration that is necessary to access the ARMC/3P for the first time.

ARMC/3P Psetup Tool

The psetup tool is used to determine the IP address assigned to the ARMC/3P by the DHCP server or to change the device's initial network configuration.

Using the Psetup Tool via Graphical User Interface

Connect the ARMC/3P to your computer via local network. Start the psetup tool, which can be found on your ARMC/3P CD, on the computer in which the ARMC/3P is installed or any other computer which is part of the same local network.

Note: If your network provides a properly configured DHCP server the ARMC/3P should be automatically assigned an IP address. Please ask your DHCP admin for the IP address the ARMC/3P got from the DHCP server.

A window opens as seen in Figure 17 (on a Windows OS) and Figure 18 ARMC/3P Psetup Tool (Linux Version).

Downloaded from www.Manualslib.com manuals search engine

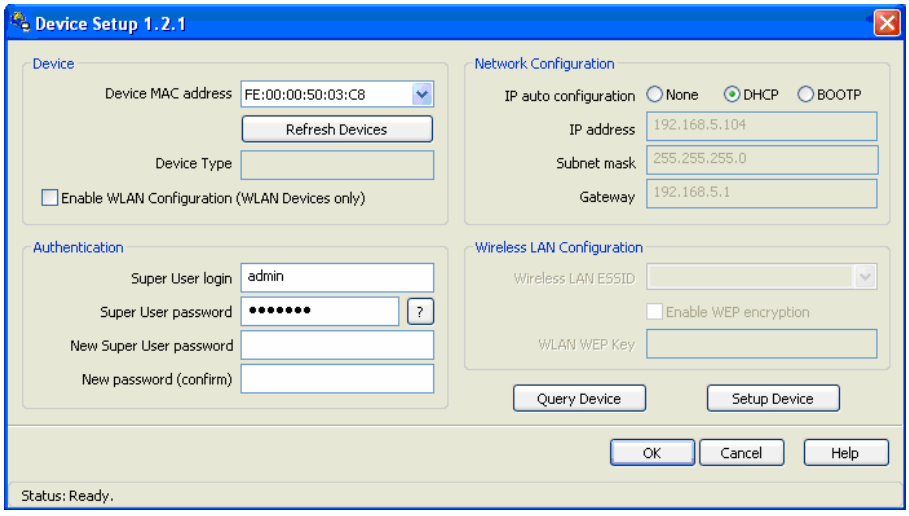


Figure 17 ARMC/3P Psetup Tool (Windows Version)

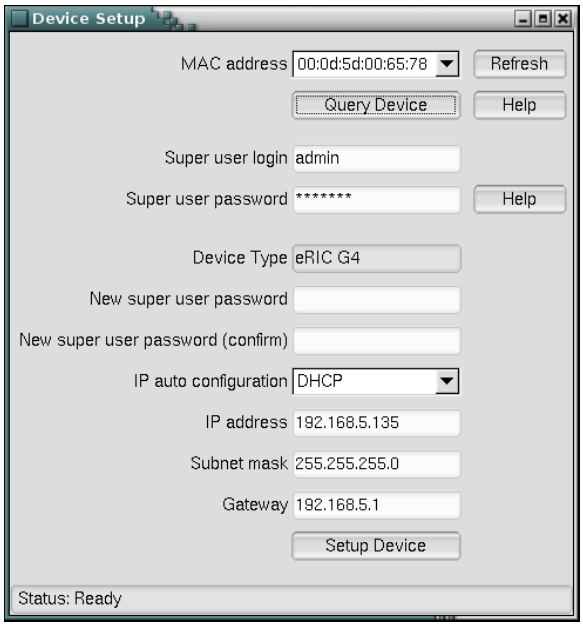


Figure 18 ARMC/3P Psetup Tool (Linux Version)

Running the Linux Psetup Tool via Command Line

The following list shows the command syntax and their usage:

--mac <MAC address of the device>
Shows the current network configuration.

--ip <neue IP address>
Set a new IP address.

Downloaded from www.Manualslib.com manuals search engine

--ipacp <dhcp|bootp|none>
Set the auto configuration.

--netmask <net mask>
Set a new netmask.

--gateway <gateway address>
Set a new gateway address.

--login <username>
Admin rights are required to change the network configuration.

--pw <password>
Password of the specified above user.

--pw-new <password>
The specified above user get a new password.

An example shows the described commands and their effects:

Displaying the current network settings

```
test@teststation:~# /home/test/psetup --mac 00:0D:5D:00:65:78
IP auto configuration: dhcp
IP address: 192.168.5.135
Subnet mask: 255.255.255.0
Gateway: 192.168.5.1
test@teststation:~#
```

Changing the network settings

```
test@teststation:~# /home/test/psetup ↵
--mac 00:0D:5D:00:65:78 --ipacp none ↵
--ip 192.168.5.55 --gateway 192.168.5.1 ↵
--netmask 255.255.255.0 --login super --pw pass
Device configured successfully.
test@teststation:~#
```

Downloaded from www.Manualslib.com manuals search engine

Mac Address Detection

Using the Psetup Tool for Windows

On the upper left corner, the MAC address of the ARMC/3P is displayed. To detect the MAC address manually, press the button **Refresh Devices**. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the ARMC/3P. On the lower right corner of the window, there are two buttons: **Query Device** and **Setup Device**. Press the **Query Device** button to display the preconfigured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter an user name and an according password. Then press the **Setup Device** button.

Using the Linux Psetup Tool

On the top of the window the MAC address of the device is displayed. To detect the MAC address manually, press the button **Refresh**. The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the ARMC/3P. Furthermore, there are two buttons on the window: **Query Device** and **Setup Device**. Press the **Query Device** button to display the preconfigured values of the network configuration. The values are displayed in the text fields located nearby. If necessary, adjust the network settings to your needs. To save the changes enter an user name and an according password. Then press the **Setup Device** button.

Authentication

To adjust the authentication settings, enter your login as a super user and change your password.

Super user login

Enter the login name of the super user. The initial value is “admin”.

Super user password

Enter the current password for the super user. This initial value is “password”.

New super user password

Enter the new password for the super user.

New password (confirm)

Re-type the new password for the super user.

To close the window and accept the changes press the **OK** button, otherwise press the **Cancel** button (on Windows). On a Linux system close the window by the appropiate button of the window frame.

Downloaded from www.Manualslib.com manuals search engine

Initial Configuration via DHCP Server

By default, the ARMC/3P will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the ARMC/3P. You can find the MAC address on the outside of the shipping box and on the bottom side of the ARMC/3P. If this initial configuration does not meet your local requirements, use the psetup tool to adjust the values to your needs. The psetup tool can be found on your ARMC/3P CD. You can follow the procedure described below.

Initial Configuration via Serial Console

To configure the ARMC/3P via serial interface both a serial port replicator cable and a null modem cable are required. Using a serial terminal, the ARMC/3P has a serial line interface (rear bracket). This connector is compliant with the RS 232 serial line standard. To establish a serial connection use a standard NULL-Modem cable. The serial line has to be configured with the parameters given in Table 5. When configuring with a serial terminal, reset the ARMC/3P and immediately press the **ESC** key. You will see some device information, and a "=>" prompt. Enter **config**, press **Enter** and wait for a few seconds for the configuration questions to appear.

Table 5 Serial Line Parameters

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	Hardware

As you proceed, the following questions will appear on the screen. To accept the default values which are shown in square brackets below, press **Enter**.

```
IP auto configuration (none/dhcp/bootp) [dhcp]:
IP [none]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:
```

IP autoconfiguration

With this option you can specify whether the ARMC/3P should get its network settings from a DHCP or BOOTP server. For DHCP, enter "dhcp", and for BOOTP enter "bootp". If you do not specify any of these, the IP autoconfiguration is disabled and subsequently you will be asked for the following network settings.

Downloaded from www.Manualslib.com manuals search engine

IP address
The IP address the ARMC/3P uses. This option is only available if IP autocon- figuration is disabled.

Net mask
The net mask of the connected IP subnet. This option is only available if IP autoconfiguration is disabled.

Gateway address
The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP autoconfiguration is disabled.

Finally, you will be asked if the values are correct, and may adjust them if necessary. After your confirmation the ARMC/3P performs a reset using the new values.

Web Interface

The ARMC/3P may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the ARMC/3P into your web browser. The initial login settings are:

Table 6 Standard User Settings

Parameter	Value
Login	admin
Password	password

Changing these settings to user specific values is strongly recommended and can be done on the “User Management” page (see **Chapter 5: User and Groups**).

Mouse, Keyboard and Video configuration

Between the ARMC/3P and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2. The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections.

ARMC/3P USB interface

To use the USB interface a correct cabling between the managed host and the managing device is necessary. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only, then you will have no remote keyboard access during the boot process of the host. Please see **Chapter 5: Keyboard/Mouse** for more details.

Downloaded from www.Manualslib.com manuals search engine

ARMC/3P Keyboard Settings

The ARMC/3P settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. Check the settings in the ARMC/3P front-end. See **Chapter 5: Keyboard/Mouse** for details.

Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The ARMC/3P addresses this situation with an intelligent synchronization algorithm. There are three mouse modes available on the ARMC/3P.

Auto Mouse Speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed Mouse Speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to n pixel moves on the remote system. This parameter n is adjustable with the scaling. It should be noted that this works only when mouse acceleration is turned off on the remote system.

Single/Double Mouse Mode

This mode is described in the Section called Single and Double Mouse Mode.

Auto Mouse Speed and Mouse Synchronization

The automatic mouse speed mode performs the speed detection during mouse syn- chronization. Whenever the mouse does not move correctly, there are two ways for re-synchronizing local and remote mouse:

Fast Sync

The fast synchronization is used to correct a temporary but fixed skew. Choose this option from the Remote Console Options menu (entry: Mouse Handling). If defined you may also press the mouse synchronization hotkey sequence (see **Chapter 4: Remote Console Control Bar** details) .

Intelligent Sync

If the Fast Sync does not work or the mouse settings have been changed on the host system, use the Intelligent Synchronization, instead. This method adjusts the parameters for the actual movement of the mouse pointer so that the mouse pointer is displayed at the correct position on the screen. This method takes more time than the Fast Sync and can be accessed with the appropriate item in the Remote Console Option menu (entry: Mouse Handling).

The Intelligent Synchronization requires a correctly adjusted picture. Use the Auto Adjustment function or the manual correction in the Video Settings panel to setup the picture.

Downloaded from www.Manualslib.com manuals search engine

Furthermore, the shape of the mouse pointer has a significant influence on the pointer detection. We recommend to use a simple, but common pointer shape. In most cases, the detection and synchronization of animated pointer shapes is likely to fail. In general, pointer shapes that change during the pointer detection process are rather impossible to figure out in the transferred video picture. With the usage of a standard mouse pointer shape the detection is rather simple and the syncronization is at its best.

Figure 19 Remote Console Control Bar: Sync Button

The **Sync Mouse** button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a Fast Sync, except in situations where the KVM port or the video mode changed recently. See also **Chapter 4: Remote Console Control Bar**.

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

Host System Mouse Settings

The host's operating system knows various settings for the mouse driver.

Important: The following limitations do not apply in case of USB and Mouse Type "MS Windows 2000 and newer".

While the ARMC/3P works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations which may prevent this synchronization from working properly:

Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows 2003 Server/XP Mouse Settings

Windows XP knows a setting named "improve mouse acceleration" which has to be deactivated.

Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled, do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

See also the **Section Recommended Mouse Settings** for mouse mode recommendations.

Downloaded from www.Manualslib.com manuals search engine

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. The mouse will be resynchronized. If resynchronizing fails, disable the mouse acceleration and repeat the procedure.

Single and Double Mouse Mode

The information above applies to the Double Mouse Mode where remote and local mouse pointers are visible and need to be synchronized. The ARMC/3P also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the Remote Console (see **Chapter 4: Remote Console Control Bar**) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

Recommended Mouse Settings

For the different operating systems on the host we can give the following advice:

MS Windows NT4

NT4 supports PS/2, only. Please choose the options PS/2 mouse and Auto Mouse Speed.

MS Windows 2000, 2003, XP (all versions)

In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option “enhance pointer precision” in the Control Panel.

Note: The remote mouse is always synchronized with the local mouse if selecting the option “MS Windows 2000 or newer”.

SUN Solaris

Adjust the mouse settings either via “xset m 1” or use the CDE Control Panel to set the mouse to “1:1, no acceleration”. As an alternative you may also use the Single Mouse Mode.

MAC OS X

We recommend using the Single Mouse Mode.

OS/2

We recommend using the Single Mouse Mode.

Linux

First, choose the option “Other Operating Systems” from the the Mouse Type selection box. Second, choose the option Auto Mouse Speed. This applies for both USB and PS/2 mice.

Note: For connecting a PS/2 mouse the PS/2 system cable is required.

Downloaded from www.Manualslib.com manuals search engine

Video Modes

The ARMC/3P recognizes a limited number of common video modes. When running X11 on the host system please do not use any custom modelines with special video modes. If you do, the ARMC/3P may not be able to detect them. We recommend using any of the standard VESA video modes instead. Please refer to **Appendix B: ARMC/3P Video Modes** for a list of all supported video modes.

Resetting the ARMC/3P to its Factory Settings

Using the S2D Pins

The ARMC/3P has two reset pins as described in **Chapter 2: The Set to Default (S2D) Pins**. Upon delivery these pins are open. Close the pins with a jumper and reboot the ARMC/3P. Wait for about two or three minutes until the primary step for the reinitialization succeeded. Remove the jumper from the Reset Pins and reboot the ARMC/3P, again. Now, you may use the default settings as described in **Chapter 3: The Initial Configuration**.

Using the Serial Interface

Reset the ARMC/3P and immediately press the **ESC** key. On your screen a command prompt "=>" will be visible. Enter the command "defaults", press the **Enter** key and wait for a few seconds for the ARMC/3P to reboot. Now, you may use the default settings as described in **Chapter 3: Initial Configuration**.

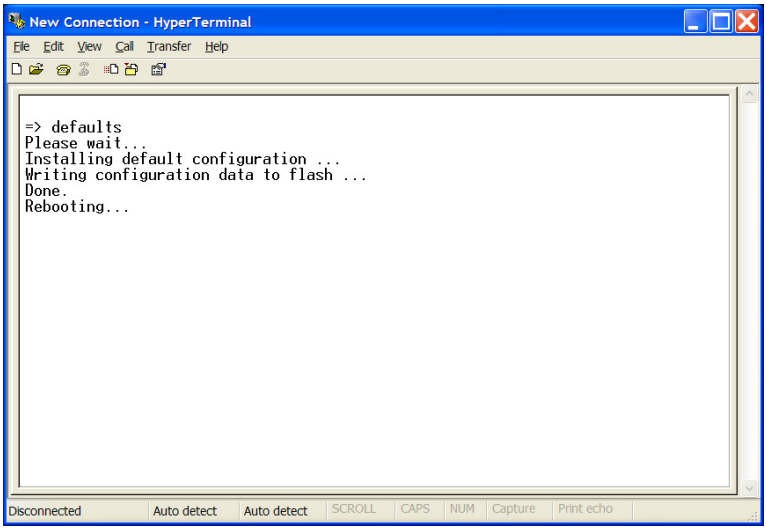


Figure 20 Terminal with Reset Message

Downloaded from www.Manualslib.com manuals search engine

Chapter 4: Usage

Prerequisites

The ARMC/3P features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the built-in Ethernet adapter or a modem, too.

The following interfaces are supported:

HTTP/HTTPS

Full access is provided by the embedded web server. The ARMC/3P environment can be entirely managed using a standard web browser. You can access the ARMC/3P using the insecure HTTP protocol or using the encrypted HTTPS protocol. Whenever possible use HTTPS.

Telnet

A standard Telnet client can be used to access ay device connected to the ARMC/3P's serial port via a terminal mode.

SSH

The ARMC/3P also offers SSH (Secure Shell) access as a secure alternative to Telnet.

The primary interface of the ARMC/3P is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Important: We recommend to install a Sun JVM 1.5.

For an insecure connection to the ARMC/3P we can recommend the following web browsers:

- Microsoft Internet Explorer version 5.0 or higher on Windows 98, Windows ME, Windows 2000 and Windows XP
- Netscape Navigator 7.0, Mozilla 1.6 and Mozilla Firefox on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm.

Downloaded from www.Manualslib.com manuals search engine

Using the Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated. The dialog box contains a link that leads you to Usage information on how to upgrade your browser to a state of the art encryption scheme. Figure 21 shows the dialog box presented by the Internet Explorer 6.0.

Figure 21 The Internet Explorer displaying the Encryption Key Length

Newer web browsers do support strong encryption by default.

Login into the ARMC/3P and logout

Login into the ARMC/3P

Open your web browser. Type in the address of your ARMC/3P which you configured during the installation process. The address used might be a plain IP address or a host and domain name, in case you have given your ARMC/3P a symbolic name in the DNS. For instance, type the following in the address line of your browser when establishing an unsecured connection:

http://192.168.1.22/

In order to use a secure connection type in:

https://192.168.1.22/

This will lead you to the ARMC/3P login page as shown in Figure 22.

Figure 22 Login Screen

Important: Your web browser has to accept cookies or else login is not possible.

Downloaded from www.Manualslib.com manuals search engine

The ARMC/3P has a built-in admin that has all the permissions to administer your ARMC/3P. See the following table for the default settings.

Table 7 Standard User Settings

Parameter	Value
Login	admin
Password	password

When you login for the first time on the ARMC/3P a window will open to request a password change as shown in Figure 23. The password change is to prevent unauthorized access of the host system and the ARMC/3P.

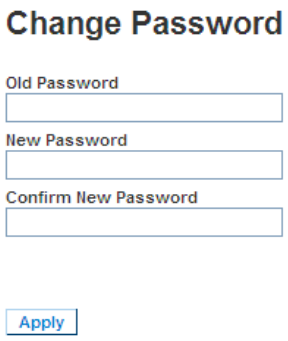


Figure 23 Password Change Request

Important: Please make sure to change the admin user password immediately after you have installed and accessed your ARMC/3P for the first time. Not changing the pass phrase for the admin user is a severe security risk and might result in unauthorized access to the ARMC/3P and to the host system including all possible consequences!

Navigation

Having logged into the ARMC/3P successfully, the main page of the ARMC/3P appears (see Figure 24). This page consists of three parts, each of which contains specific information. The buttons on the upper side allow you to switch between the different sections of the ARMC/3P (see Figure 25). The lower left frame contains user and device information (see **錯誤! 找不到參照來源。** for details). Within the right frame, task-specific information is displayed that depends on the section you have chosen before.

Downloaded from www.Manualslib.com manuals search engine

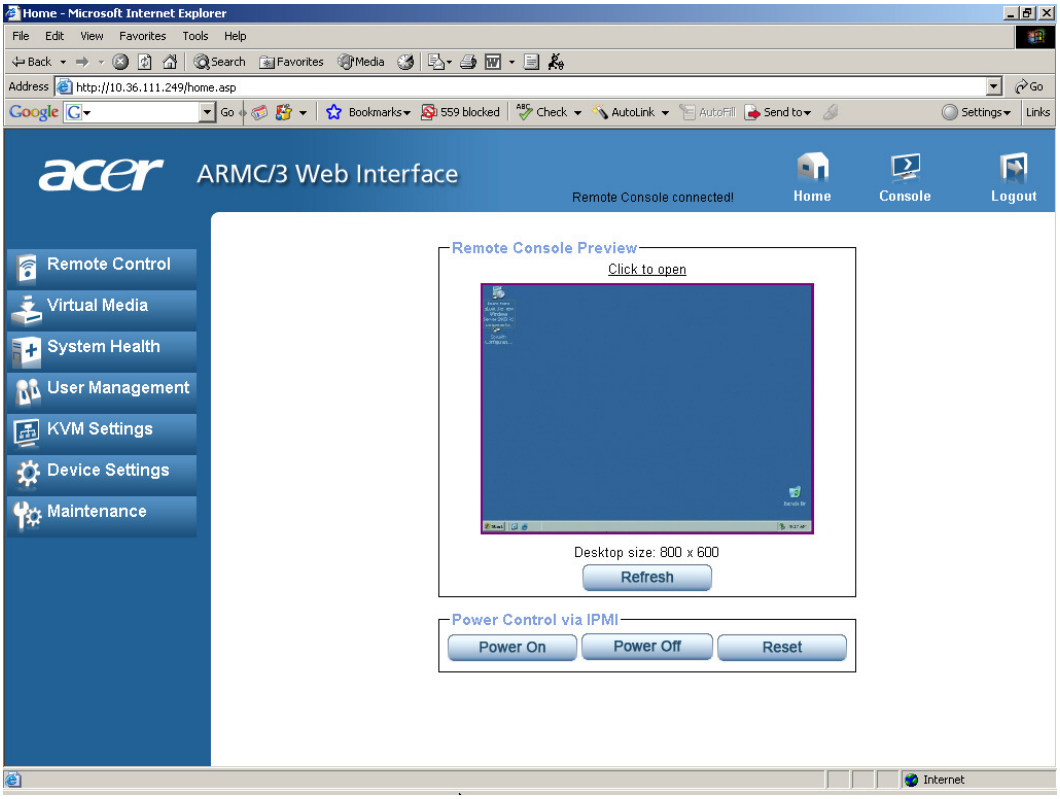


Figure 24 ARMC/3P Main Page Overview

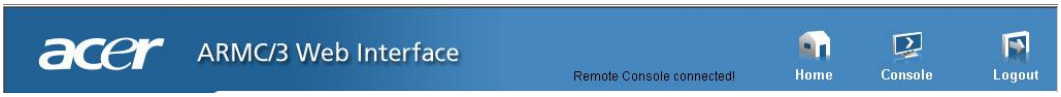
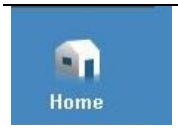


Figure 25 Navigation Frame Overview

Table 8 Links for Navigation

Link	Description
	Click to open the main page overview (like Figure 24).
	Click to open the KVM Console.

Important: If there is no activity for half an hour, the ARMC/3P will log you out automatically. A click on one of the links will bring you back to the login screen.

Downloaded from www.Manualslib.com manuals search engine

Logout from the ARMC/3P

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for half an hour.

Figure 26 Logout Link

Managing the ARMC/3P with a CommandCenter

If you use CommandCenter Secure Gateway to manage your devices, then you can add your ARMC/3P to CC-SG´s management domain to enable all CommandCenter features for ARMC/3P. This includes single sign on and central user management and will allow you to operate and configure the ARMC/3P directly from the CommandCenter. Please consult your CommandCenter manual for further information on this topic.

While the ARMC/3P is managed by a CommandCenter no local access is possible.
Access and Authorization will only be granted through the CommandCenter.

Releasing the ARMC/3P from managed mode should be done with the CommandCenter. Should the CommandCenter not be available for some reasons, then the ARMC/3P will automatically reenable local logins after a defined time. The administrator can then manually release the ARMC/3P from CommandCenter.

The Remote Console

General Description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that the ARMC/3P controls.

The Remote Console window is a Java Applet that tries to establish its own TCP connection to the ARMC/3P. The protocol that is run over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port #443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

Downloaded from www.Manualslib.com manuals search engine

In case the ARMC/3P is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the connection. This is because today's web proxies are not capable of relaying the RFB protocol.

In case of problems, please consult your network administrator in order to provide an appropriate network environment.

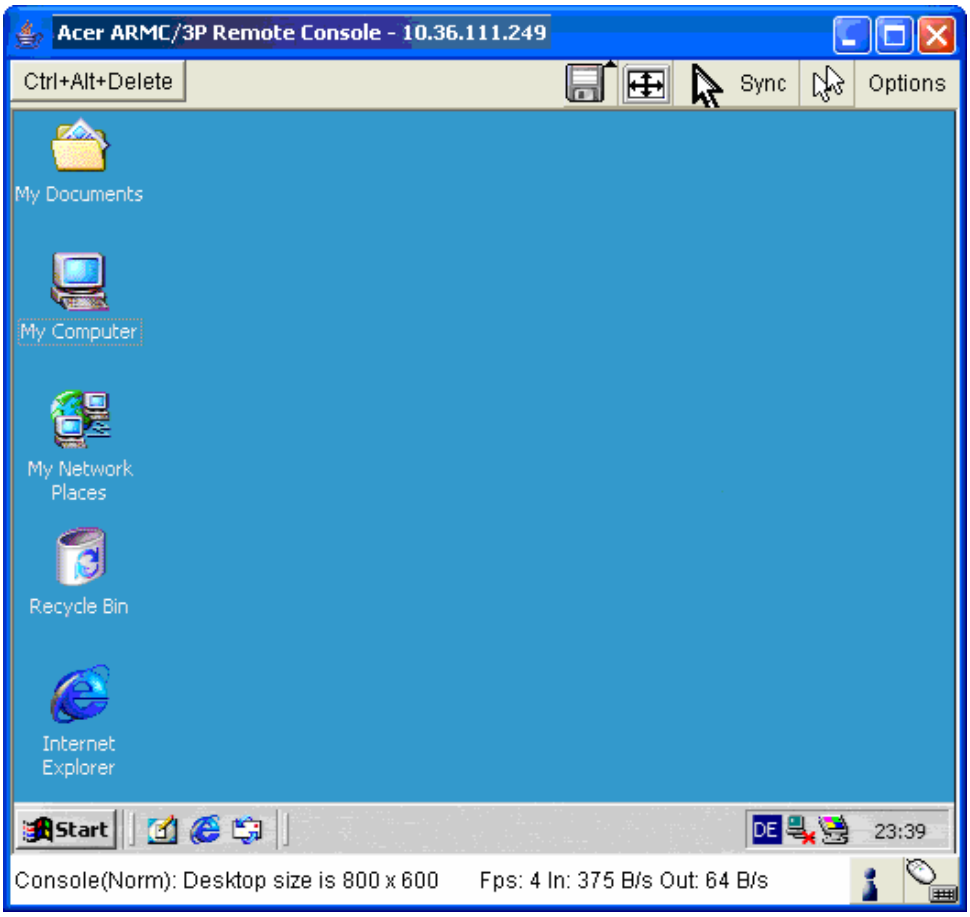


Figure 27 Remote Console

Main Window

Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the line which you use to connect to the ARMC/3P.

With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system and your host system uses a US English keyboard layout, for instance, special keys on the

Downloaded from www.Manualslib.com manuals search engine

German keyboard will not work as expected. Instead, the keys will work like their US English counterparts. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Important: In difference to the remote host system, the Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings. A description for each control follows.

Figure 28 Remote Console Control Bar

Ctrl+Alt+Delete

Special button key to send the “Control Alt Delete” key combination to the remote system (see also **Chapter 5: KVM Settings** for defining new button keys).

Drive Redirection button

Menu Button for opening the Drive Redirection menu and choosing between two virtual media options at the same time (see also **Chapter 5: Drive Redirection**).

Note: The “Drive Redirection” window with the two drives for selection opens only if the client system is using Windows 2000 or higher and if the Remote Console user has an administrator status on Windows. In case the client system is using a LINUX OS the “Drive Redirection Selection” window will not be displayed.

Auto Adjust button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the ARMC/3P tries to adjust itself for the best possible video quality.

Downloaded from www.Manualslib.com manuals search engine

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on that.

Single/Double Mouse Mode

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchonized). Single Mouse Mode is only available if using SUN JVM 1.4 or higher.

Note: If the "Host Interface" is set on "USB" and the "USB Mouse Type" is set on "Windows >= 200, MAC OS X" then the buttons for "Sync Mouse" and "Single/Double Mouse Mode" are hide.

Options

To open the Options menu click on the button **Options**. See the **Section Remote Console Options** for a detailed description of the available options for the ARMC/3P.

Remote Console Options

To open the Options menu click on the button **Options**.

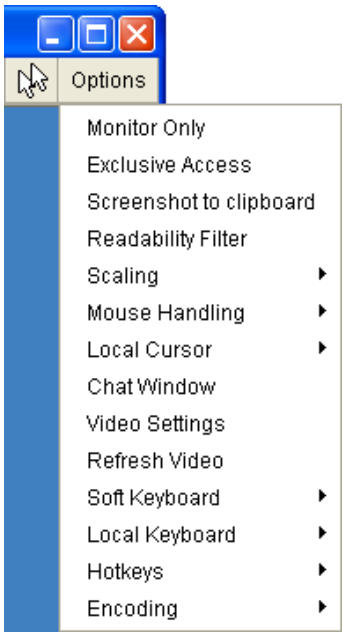


Figure 29 Remote Console Options Menu

A description of the options follows.

Downloaded from www.Manualslib.com manuals search engine

Monitor Only

Toggles the Monitor Only filter on or off. If the filter is switched on no remote console interaction is possible. The remote screen can be viewed, only.

Exclusive Access

If a user has the appropriate permission, he or she can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off. A change in the access mode is also visible in the status line. See the **Section Remote Console Status Line** for more information.

Readability Filter

Toggles the Readability Filter on or off. If the filter is switched on in scaling mode, it will preserve most of the screen details even if the image is substantially scaled down. This option will be available only with a JVM 1.4 or higher.

Scaling

Allows you to scale down the Remote Console. You can still use both mouse and keyboard, but the scaling algorithm will not preserve all display details.

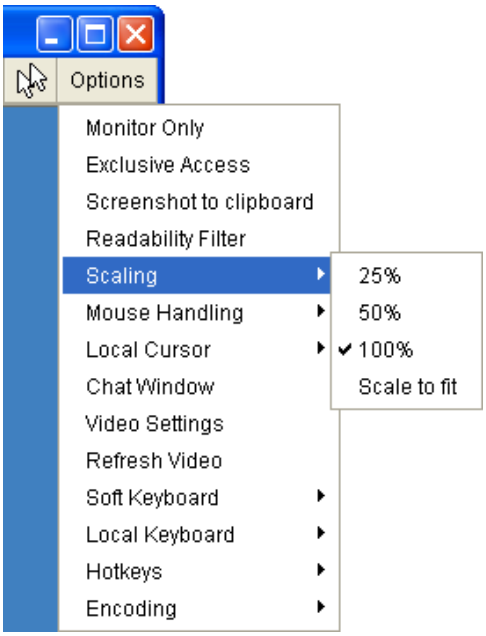


Figure 30 Remote Console Options Menu: Scaling

Downloaded from www.Manualslib.com manuals search engine

Mouse Handling

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer as explained in **Chapter 3: Mouse, Keyboard and Video configuration**.

- Fast Sync
  The fast synchronization is used to correct a temporary but fixed skew.

- Intelligent Sync
  Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

- Mouse Mode
  Use this option to choose between Single Mouse or Double Mouse Mode, see **Section: Remote Console Control Bar**.

Important: This method takes more time than the fast one and requires a correctly adjusted picture. To setup the picture you may use either the auto adjustment function or the manual correction in the Video Settings panel.

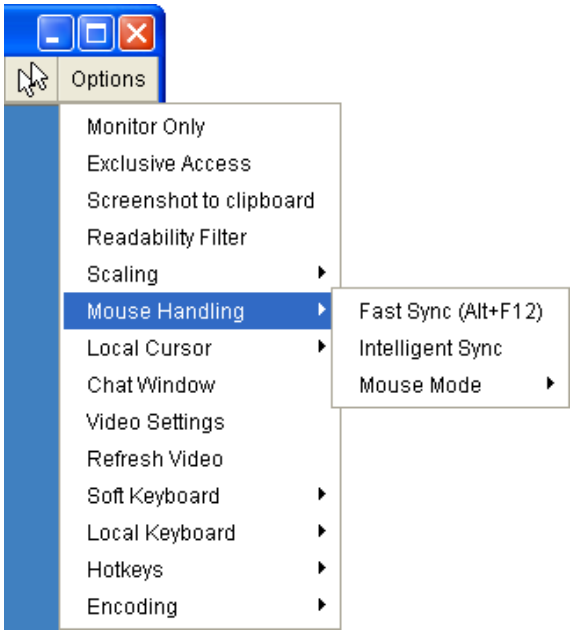


Figure 31 Remote Console Options Menu: Mouse Handling

Local Cursor

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine, a version of 1.2 or higher offers the full list.

Downloaded from www.Manualslib.com manuals search engine

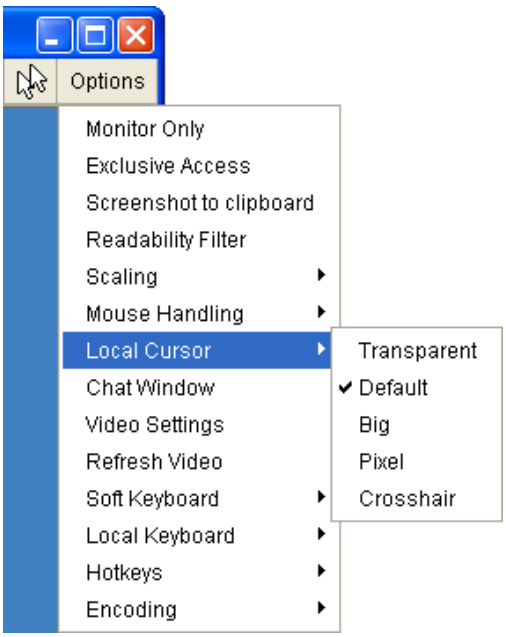


Figure 32 Remote Console Options Menu: Local Cursor

Chat Window

The ARMC/3P Remote Console features a Chat Frame that allows you to communicate with other parties logged into the same card. Figure 33 Remote Console Options Menu: Chat Window shows an example of the Chat Frame.

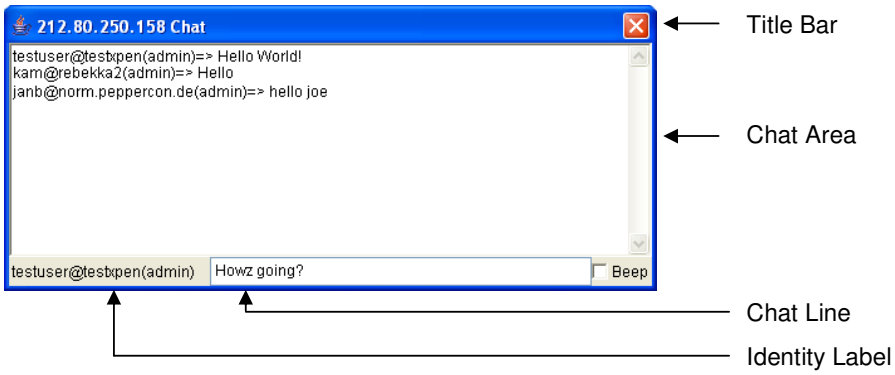


Figure 33 Remote Console Options Menu: Chat Window

The Chat Frame is helpful especially for discussing problems and questions among the users logged into the ARMC/3P. The remote host's screen should not be changed or misused for that purpose.

Title Bar

Shows the IP address of the ARMC/3P you are connected to.

Downloaded from www.Manualslib.com manuals search engine

Chat Area

Read-only text area showing the messages, which have been received so far, including your own messages sent to others. The identity string of the sender precedes each message.

Identity Label

Shows the identity string used to precede messages sent by this Chat Frame. The first part of the identity string is the user ID that has been used to log into the client system, i.e. the system the browser runs on. The second part, behind the " @ ", is the hostname of the client system. The last part in round brackets is the user who logged into the ARMC/3P . As displayed in Figure 33, it is the user "super" .

Chat Line

This is an editable text line, where a new message can be entered. Once the **Enter** key is hit the message is broadcasted to every other connected party. In case a connected user has not yet opened the Chat Frame, it will be opened automatically in order to receive and display the delivered message.

Important: Any message sent to the Chat will be broadcasted to all connected users, which are using the Remote Console at the time the message was sent. There is no option to direct a message to a particular user only. The Chat has no message history. That means, messages will be received only after opening the Remote Console. Messages that possibly have been sent among other users will be lost for a user who opens up his Remote Console afterwards.

Video Settings

Opens a panel for changing the ARMC/3P video settings. The ARMC/3P features two different dialogs which influence the video settings.

Video Settings through the HTML Frontend

Select this option to enable local video port. This option decides if the local video output of the ARMC/3P is active and passing through the incoming signal from the host system.

The option Noise Filter defines how the ARMC/3P reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Settings through the remote console

Downloaded from www.Manualslib.com manuals search engine

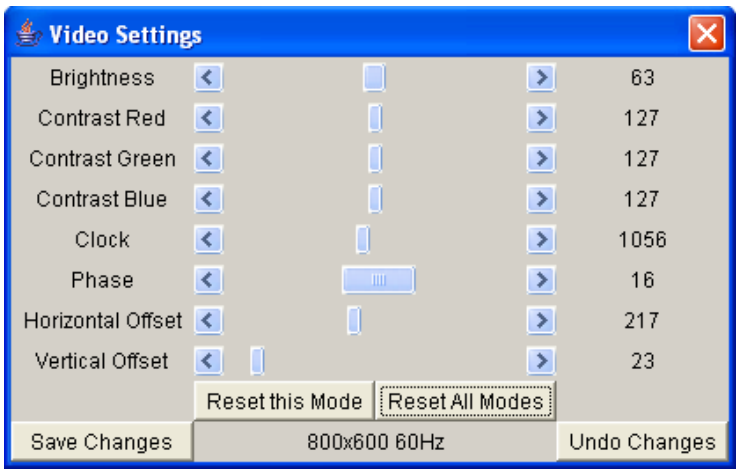


Figure 34 Remote Console Options Menu: Video Settings Panel

Brightness
Controls the brightness of the picture.

Contrast
Controls the contrast of the picture.

Clock
Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. To achieve a better picture quality you may try to change this setting together with the sampling phase.

Phase
Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.

Horizontal Position
Use the left and right buttons to move the picture in horizontal direction while this option is selected.

Vertical Position
Use the left and right buttons to move the picture in vertical direction while this option is selected.

Reset this Mode
Reset mode specific settings to the factory-made defaults.

Reset all Modes
Reset all settings to the factory-made defaults.

Save changes
Save changes permanently.

Downloaded from www.Manualslib.com manuals search engine

Undo Changes

Restore last settings.

Refresh Video

Use this option to refresh the video picture. The video data for the Remote Console is updated completely.

On startup of the Remote Console, the ARMC/3P transmits the entire video picture from the remote host. Subsequently, the parts of the video picture that did not change are filtered and not transmitted, again. This leads to less video data to be transmitted. It may happen that there are parts of the video picture that are not updated correctly (video noise, compression errors). You may use this option to initiate an entire refresh, manually.

Soft Keyboard

The Soft Keyboard simulates an entire keyboard that is connected to the remote system. It is necessary in case your remote system runs with a completely different language and country mapping than your administration machine. By selecting the appropriate button(s) you can send key codes and also key sequences to the remote system and act as if you would work with a keyboard that is directly connected to the remote system.

In order to open the Soft Keyboard select the entry “Soft Keyboard” from the **Options** menu. You can send single key strokes like F as well as combinations of keys such as `Ctrl+C` or `AltGr+Shift+F4`.

For a single key stroke you can click on the button with the appropriate character. Single keys such as regular characters and numbers are sent immediately. Special keys like `Ctrl`, `Shift` as well as the function keys `F1` to `F12` have to be selected twice. The first press sends the signal “key is pressed”, the second press sends the signal “key is released” to the remote system. After the first press the button will change its color to indicate that the appropriate key is pressed, currently. After the second press the button will appear as usual and indicate that the key was sent.

To send the key combination `Ctrl+C` select the button `Ctrl` first. The button will change its color. Press the button `C`. The following key (`C` in our example) will be combined with the previously selected key. Both the buttons `Ctrl` and `C` are released and the key combination will be sent to the remote system. The button `Ctrl` will appear as normal (color change).

In order to send the key combination `Ctrl+F5` three steps have to be taken. Select the button `Ctrl` once and the button `F5` twice. The last press will release both buttons and send the key combination to the remote system.

In order to send the key combination `AltGr+Shift+F4` four steps are required. First, select the button AltGr once. Second, select the button Shift. Finally, choose the button `F4` twice. The last press will release all the buttons and send the key combination to the remote system.

Acer ARMC/3P English (United States) 104pc
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prn Brk
` 1 2 3 4 5 6 7 8 9 0 - = ← In / * -
q w e r t y u i o p [ ] Del End 5 +
a s d f g h j k l ; ' \
\ z x c v b n m , . / End
Ctrl St Alt Alt St Me Ctrl Ins De

Downloaded from www.Manualslib.com manuals search engine

Figure 35 Remote Console Options Menu: Softkeyboard

- Show
  Displays the Soft Keyboard.

- Mapping
  Used for choosing the appropriate language and country mapping of the Soft Keyboard.

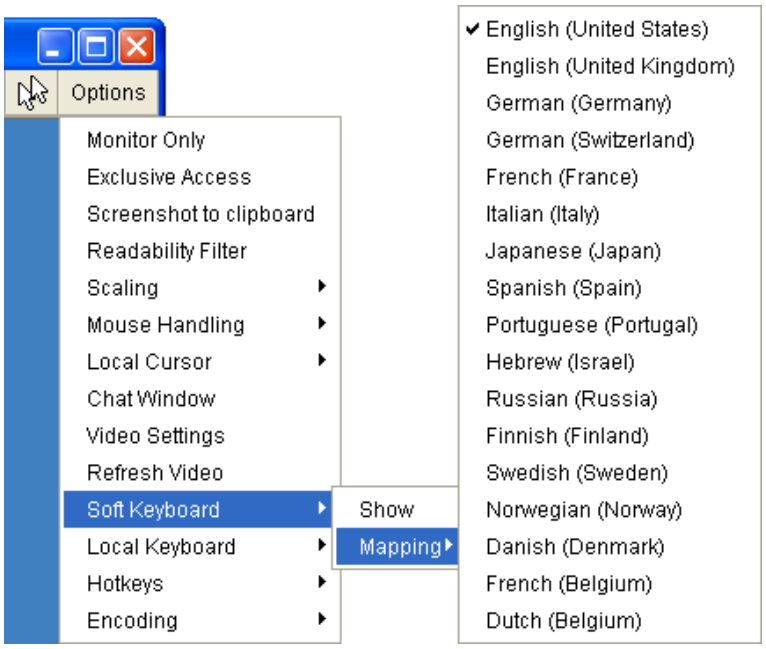


Figure 36 Soft Keyboard Mapping

Local Keyboard

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses a US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language manually.

Hotkeys

Opens a list of hotkeys defined before. In order to send a registered command to the host system choose the appropriate entry. A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Choose **OK** to perform the command on the remote host. For a detailed description see **Chapter 5: Remote Console Button Keys**.

Downloaded from www.Manualslib.com manuals search engine

Figure 37 Remote Console Options Menu: Hotkey Confirmations Dialog

Encoding

These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless “Transmission Encoding” is determined automatically (see **Chapter 5: Transmission Encoding**).

- Predefined
  This option **Predefined** offers optimized data for transmission. It depends on the bandwidth of the chosen connection.

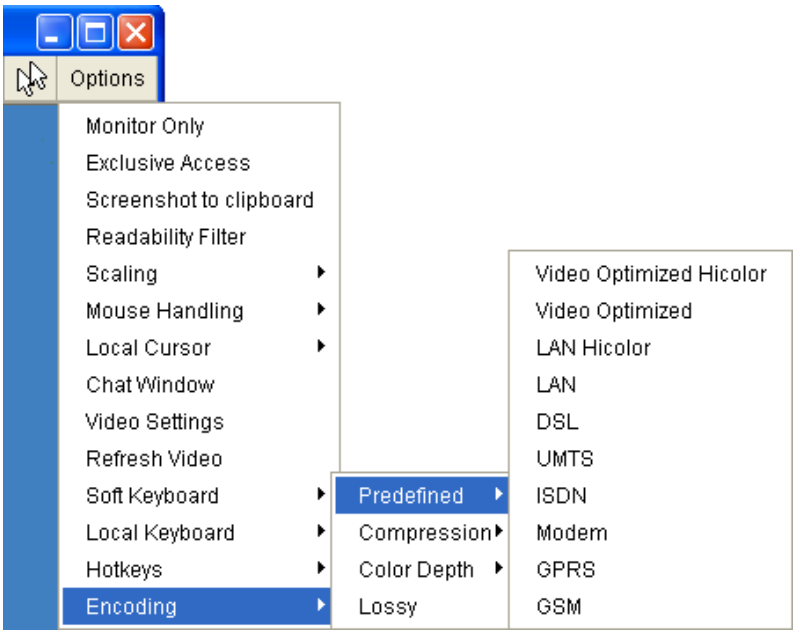


Figure 38 Remote Console Options Menu: Encoding - Predefined

- Compression level
  You may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression. The most suitable compression level should always be seen as a compromise between the network bandwith that is available, the video picture to be transferred, and the number of changes between two single video pictures. We recommend to use a higher compression level if the network bandwidth is low. The higher the compression level the more time is necessary to both pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g.

Downloaded from www.Manualslib.com manuals search engine

the number of colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

If level 0 is chosen the video compression is disabled, completely.

The option **Video Optimized** has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

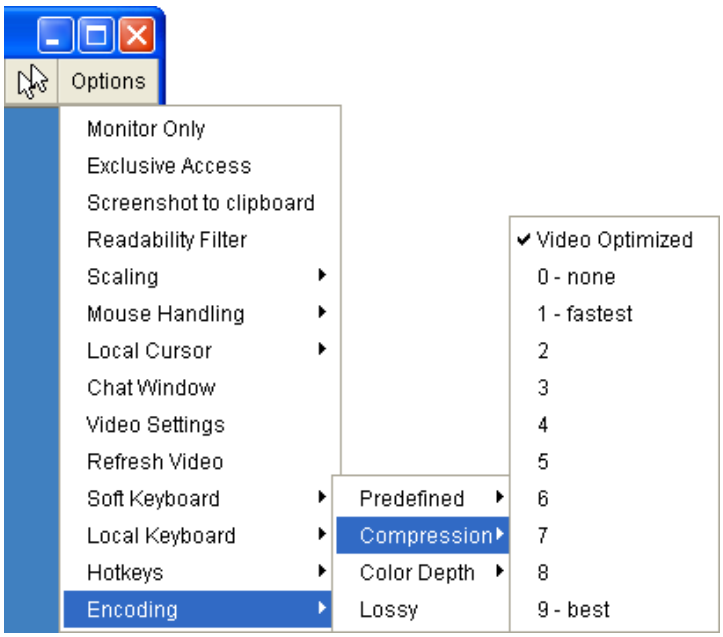


Figure 39 Remote Console Options Menu: Encoding - Compression

- Color Depth
  Set the desired color depth. You may select between 8 or 16 bit for Video Opti- mized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and transferred.

Downloaded from www.Manualslib.com manuals search engine

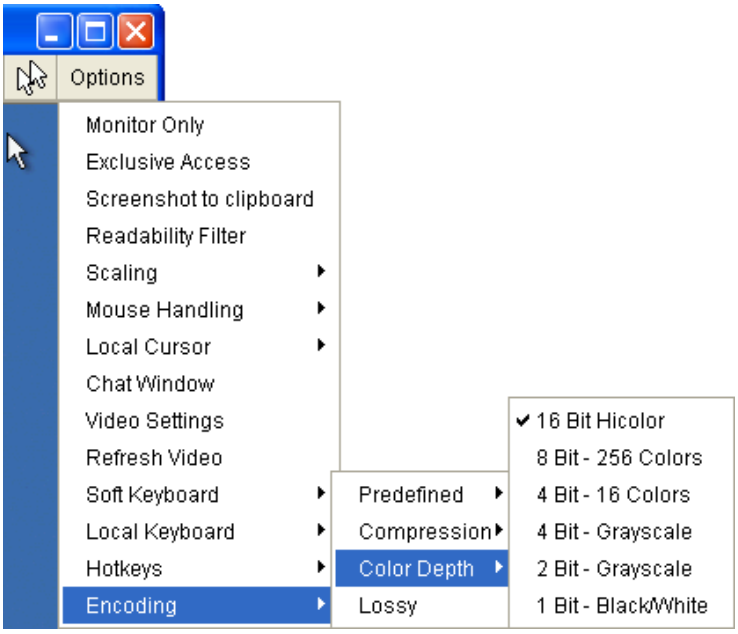


Figure 40 Remote Console Options Menu: Encoding – Color Depth

Note: If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized". As a general result, the data rate is reduced (less bits per color). Furthermore, the ARMC/3P will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

- Lossy
  Toggles the Lossy filter on or off. If the filter is switched on there will be less data transmitted but no frames/pictures lost. That means a higher frame rate with fewer details.

Remote Console Status Line

The status line shows both console and the connection state. On the left the size of the remote screen is displayed. Figure 41 was taken from a Remote Console with a resolution of 800x600 pixels (see **Appendix B:** ARMC/3P Video Modes for a list of screen resolutions that can be displayed using the ARMC/3P). The value in brackets describes the connection to the Remote Console. "Norm" means a standard connection without encryption, "SSL" indicates a secure connection using Secure Socket Layer (SSL).

Figure 41 Remote Console Status Line

The status line displays the number of frame buffer updates ("Fps") as well as the incoming ("In:") and the outgoing ("Out:") network traffic in kilobytes per second. A

Downloaded from www.Manualslib.com manuals search engine

low value of the network traffic is recommended and can be achieved as described in the **Section Optimizing the Video Picture**. If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

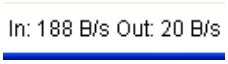


Figure 42 Status Line Transfer Rate

The next button displays the Remote Console Access settings.

Table 9 Buttons displaying the Access Status

	One single user is connected to the Remote Console of the ARMC/3P.
	One or more users are connected to the Remote Console of the ARMC/3P.
	A remote user has exclusive access. You may not access the remote host via Remote Console unless the other user disables this option.
	Exclusive access is set for you. Any other user may not access the remote host via Remote Console unless you disable this option.

The outer right button displays the state of the Monitor Only settings.

Table 10 Buttons displaying the Monitor State

	The option Monitor Only is disabled.
	The option Monitor Only is enabled.

For more information about Monitor Only and Exclusive Access settings see the according paragraphs in the Remote Console Control Bar.

Optimizing the Video Picture

To achieve an optimal video picture for the Remote Console follow the steps as given here:

1. Press the **Auto Adjust** button once (see the **Section Remote Console Control Bar** for details).

Downloaded from www.Manualslib.com manuals search engine

2. Choose the option **Video Settings** from the **Options** Menu of the Remote Console. Press the button **Reset this Mode**.

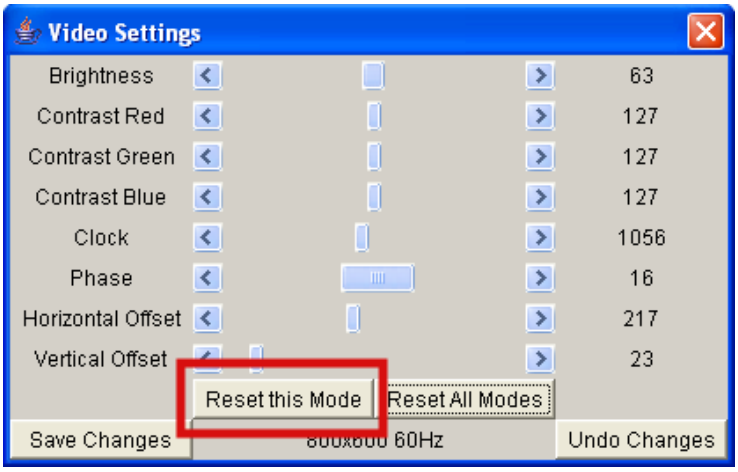


Figure 43 Remote Console Video Settings: Reset this Mode

3. Again, press the **Auto Adjust** button once.
4. The ARMC/3P detects the video mode with 8 bits (256 colors) automatically. To improve the picture quality you may select 16 bit (True Color) from the **Options** Menu of the Remote Console, sub menu “Encoding”, entry “Color Depth” (see the **Section Encoding** for details).
5. Finally, if the the Remote Console transfer rate is too high you may do an adjustment using the Noise filter. The higher the filter level the more information is filtered from the transferred video picture (see the Section called Video in Chapter 6 for details) and the data rate is reduced.

Currently, the video picture with the best quality can be achieved with the settings “16 bit (High Color)” in the Remote Console or “LAN (High Color)” in the web frontend. This option can also be preset in **Chapter 5: User Console**. The sub menu “Compression” from the Options menu has no influence on the picture quality but on the data rate of the picture that is transferred to the Remote Console.

Reducing the Noise of the Video Picture

To reduce the noise from the video picture for the Remote Console you may adjust the Noise filter. Prior to that we recommend optimizing the video picture as described in the Section called Optimizing the Video Picture.

In most cases the rate of transferred data indicates the noise level. The higher the transfer rate, the higher the noise of the video picture. You may do an adjustment using the Noise filter. The higher the filter level the more information is filtered from the transferred video picture (see **Chapter 5: Video** details) and the data rate is reduced.

Downloaded from www.Manualslib.com manuals search engine

Using the ARMC/3P with low bandwidth

The network connection of the ARMC/3P has an important influence on the time between two single video pictures. On a connection with low bandwidth it takes longer to transfer the video data from the ARMC/3P to the Remote Console on the local host. If the remote screen has changed a new picture is sent.

In terms of transfer time there is no difference between text screens and screens in graphics mode. The video picture is taken as graphics data no matter what the screen looks like and which video mode is chosen. In terms of transferred data there can be an improvement. The compression plays an important role here. You can choose a compression level from the sub menu **Compression** in the **Options** menu of the Remote Console.

Please note that the video will be compressed on the ARMC/3P, transferred to the Remote Console and unpacked in a Java environment. Depending on the remote host and on the local machine this procedure may take some time and may result in a slowly updated picture in the Remote Console.

To improve the speed you may also set the picture quality in the Remote Console to either “8 bit” or even to grayscale. Due to less video data to be processed this is likely to be more effective than the highest compression level.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Chapter 5: Menu Options

Remote Control

KVM Console

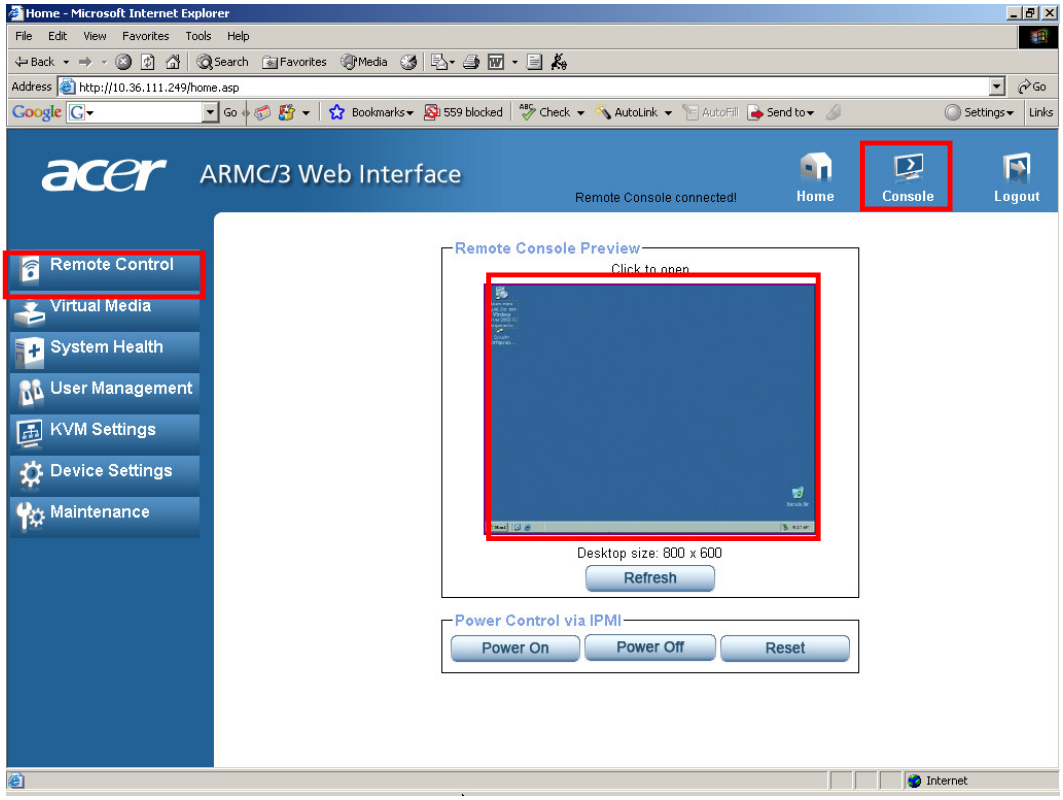


Figure 44 Main Page with Remote Console Preview

Remote Console Preview

To open the KVM console click on the **Remote Console** link on the left or on the console picture on the right, or click the **Remote Control** navigation button and choose **KVM Console** (seen in Figure 44). To refresh the picture click on the button that is named **Refresh**.

Remote Power

Use the "Remote Power" page to control the host system's power status via one of the following methods:

- Internal Power Control via ATX wires
- Power Control via IPMI

Downloaded from www.Manualslib.com manuals search engine

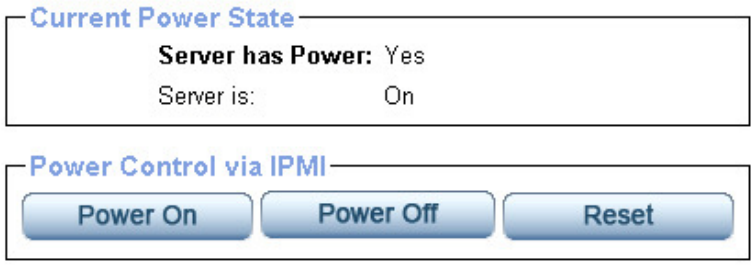


Figure 45 Power Control Overview

Internal Power Control via ATX wires

The power button is the representation of the ATX power button on your host system. It is used to switch on and off the power supply. The ATX power button knows two operation modes: pressing it shortly and pressing it for about 4 seconds.

Short Press

A short press on the ATX button is normally caught by the running operating system that tries to initiate a controlled shutdown.

Usually this should always be the first action you try in case you would like to power off your system. Only in case this is not working you should try the long press button.

Please note that after you have pressed this button the power state displayed in the administration panel will not immediately reflect the requested change. A controlled shut down of the system may take some minutes. You can observe the action caused by your button press using the Remote Console window or by reloading the Server Power Control panel.

Long Press

This will unconditionally power off the system. Even if you have submitted a short press before, this will shut down the power supply of the host system.

The effect of the long button press can be immediately observed on the panel that is loaded into the browser because of the button press. The power state will be off.

*R*eset

Pressing this button is similar to pressing the **Reset** button directly on the remote system. Be aware that pressing the **Reset** button will result in an unconditional and immediate cold start of the system. This might damage open files and the file system itself.

Figure 46 'Internal Power Control' Buttons

Downloaded from www.Manualslib.com manuals search engine

Important: The prerequisite for the remote power/reset button to work is a correct installation of the ARMC/3P.

Power Control via Intelligent Platform Management Interface (IPMI)

The ARMC/3P is capable of controlling the power status of an IPMI-enabled host system. See **Chapter 5: Intelligent Platform Management Interface (IPMI)** for configuration instructions. If the ARMC/3P is configured to act as an IPMI client the Remote Power Control page will show three buttons:

Power On
Sends an IPMI "Power On" command to the Baseboard Management Controller (BMC).

Power Off
Sends an IPMI "Power Off" command to the BMC.

Reset
Sends an IPMI "Hard Reset" command to the BMC.

Figure 47 'Power Control via IPMI' Buttons

Telnet Console

The ARMC/3P firmware features a Telnet gateway that enables a user to connect to the ARMC/3P via a standard Telnet client. For connecting to the ARMC/3P via Telnet protocol you may use a terminal program such as `xterm`, `TeraTerm` or `Putty`. As an alternative you may also enter the telnet command on the command line or use the "Run" dialog from the Windows Start Menu. As an example you may type the following sequence:

telnet 192.168.1.22

Replace the IP address by the one that is actually assigned to the ARMC/3P. This will prompt for user name and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means the user management of the Telnet interface is entirely controlled with the comparable functions of the web interface.

Once you have successfully logged into the ARMC/3P a command line will be presented and you can enter the necessarry management commands.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is acti-

Downloaded from www.Manualslib.com manuals search engine

vated (if the serial settings were made accordingly). All inputs are redirected to the device on serial port #1 and its answers are displayed on the Telnet interface.

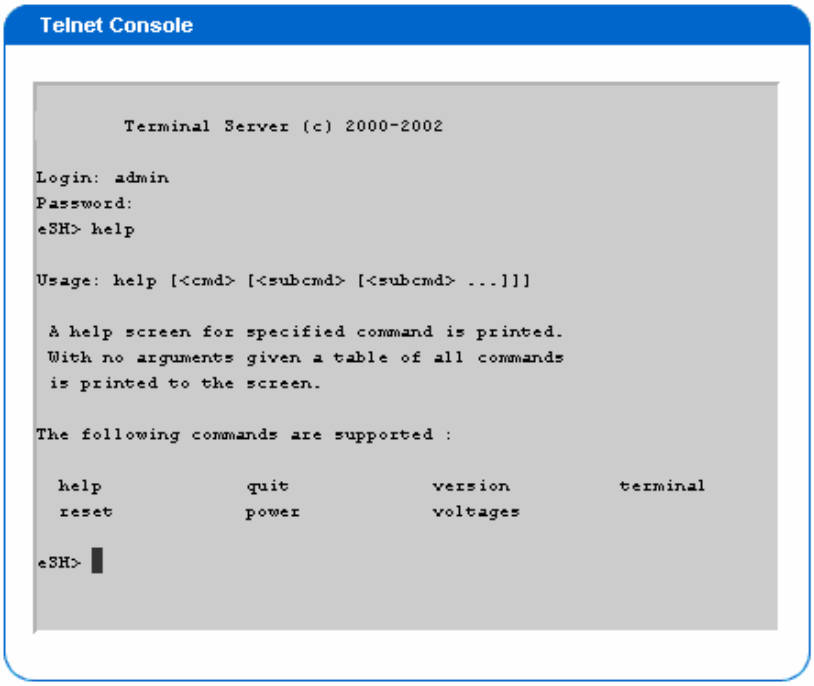


Figure 48 Telnet Console

The following list shows the command syntax and their usage.

help
Displays the list of possible commands

quit
Exits the current session and disconnects from the client

version
Displays the release information

terminal
Starts the terminal pass-through mode for serial port #1. The key sequence esc exit switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for pass-through access.

reset [host|card]
Resets the given target, the host system or the ARMC/3P card. If no reset target is given it defaults to “host”. Note that resetting the ARMC/3P results in disconnecting every client. This includes also the client the reset command was sent from.

power [on|off [short|long]]
The host is powered on or off. If no new power state is given, the current

Downloaded from www.Manualslib.com manuals search engine

state will be displayed. The given attribute (either short or long) will determine the ATX duration. The default value is short.

Voltages

Displays a list of all current voltages of the system.

Downloaded from www.Manualslib.com manuals search engine

Virtual Media

The ARMC/3P provides Double Virtual Media. So it is possible to choose between two virtual media devices at the same time, for example required by special applications like BOOT procedure.

Floppy Disk

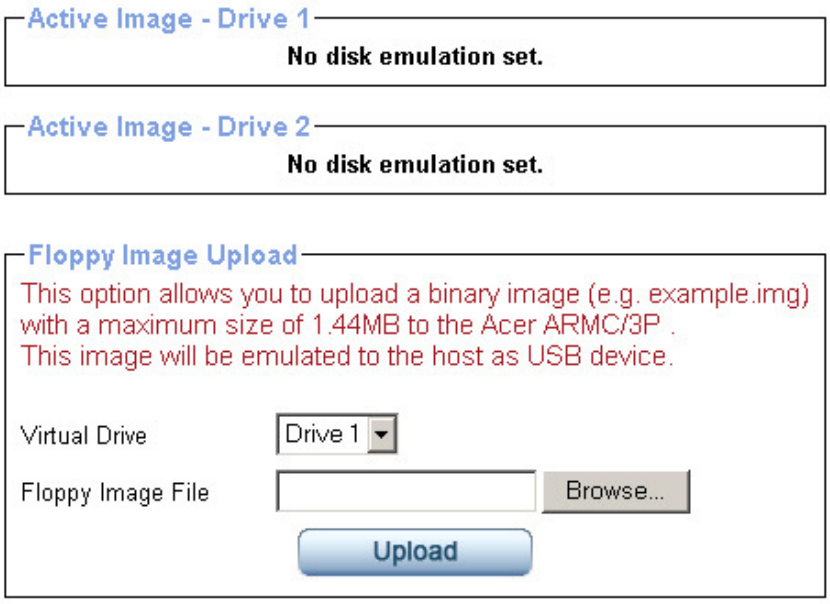

Active Image - Drive 1
No disk emulation set.
Active Image - Drive 2
No disk emulation set.
Floppy Image Upload
This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the Acer ARMC/3P .
This image will be emulated to the host as USB device.
Virtual Drive
Drive 1
Floppy Image File
Browse...
Upload

Figure 49 Floppy Virtual Area

Upload a Floppy Image

With two small steps working on the basis of a certain (floppy) image can be achieved.

- First the path of the image has to be specified. You can do that either by hand or by using the file selection dialog of your web browser. To open the file selection dialog click on the **Browse** button and select the desired image file.

  The maximum image size is limited to 1.44MB. To use a larger image mount this image via Windows Share (or SAMBA) (see the Section called Use Image on Windows Share (SAMBA) for details).

- Secondly, click on the **Upload** button to initiate the transfer of the chosen image file into the ARMC/3P's on-board memory. This image file is kept in the on- board memory of the ARMC/3P until the end of the current session, until you logged out or initiated a reboot of the ARMC/3P.

Downloaded from www.Manualslib.com manuals search engine

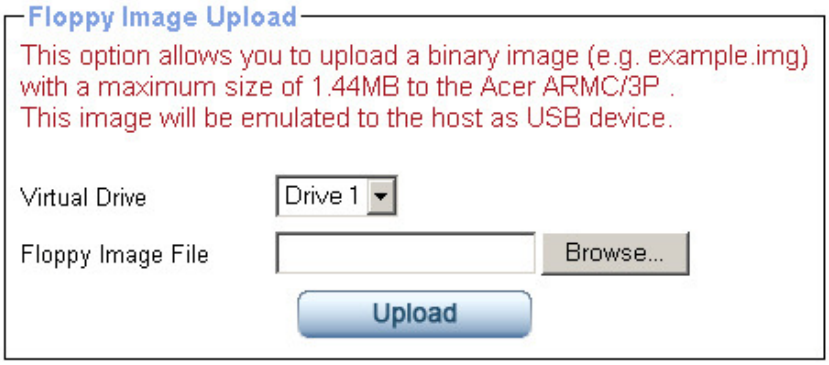

Floppy Image Upload
This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the Acer ARMC/3P .
This image will be emulated to the host as USB device.
Virtual Drive
Drive 1
Floppy Image File
Browse...
Upload

Figure 50 Select Image File

Download a Floppy Image

A floppy image kept in the ARMC/3P's memory can be both read and written to. To retrieve the changed image contents after writing to it click the **Download** button and select a folder to store the file in.

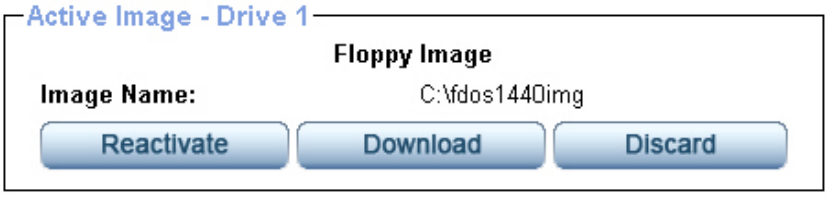


Figure 51 Active Image File

CD ROM

Use Image on Windows Share (SAMBA)

To include an image from a Windows share select **CD-ROM** from the submenu. The following information has to be given to mount the selected image properly:

Share host
The server name or its IP address. On Windows 95, 98 and Windows ME do not specify the IP address but the server name ("NetBIOS Name").

Share name
The name of the share to be used.

Path to image
The path of the image file on the share.

User (optional)
If necessary, specify the user name for the share named before. If

Downloaded from www.Manualslib.com manuals search engine

unspecified and a guest account is activated, this guest account information will be used as your login.

Password (optional)
If necessary, specify the password for the given user name.

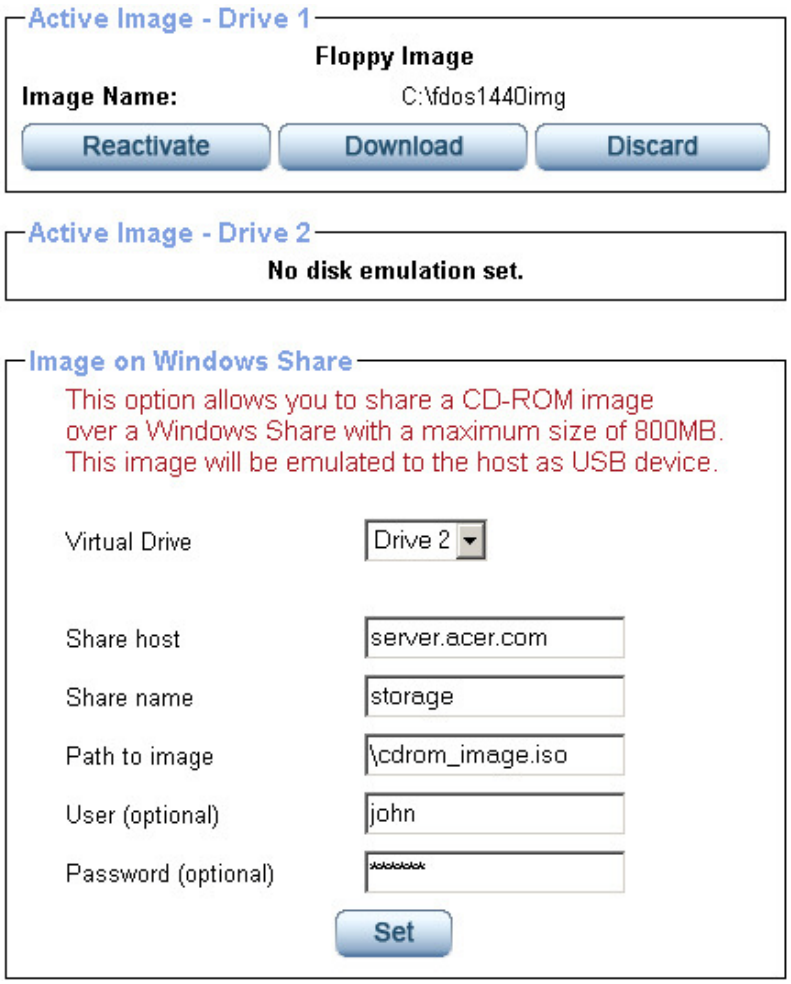


Figure 52 Selecting CD-ROM and Windows Share

For an example you may have a look on Figure 52. First, the ARMC/3P will look for a server named mysql.acme.com. Then, the entered share name is selected (in our example we use the share storage) and the image file \cdrom_image.iso is opened. If this file can only be accessed with both a user name and password enter the appropriate values in the input fields for user name and password. In our case the file is owned by the user “johndoe” and protected by a user-specific pass-phrase (displayed as a number of stars).

To register the specified file image and its location click on the Set button.

Downloaded from www.Manualslib.com manuals search engine

The specified image file is supposed to be accessible from the ARMC/3P. The information above has to be given from the point of view of the ARMC/3P. It is important to specify correct IP addresses and device names. Otherwise, the ARMC/3P may not be able to access the referenced image file properly, leave the given file unmounted and it will display an according error message, instead. So, we recommend to state correct values and repeat this step if necessary.

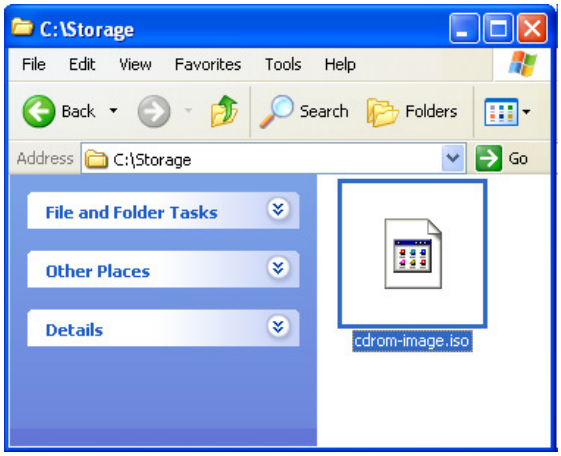


Figure 53 The Image File on the Share

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as “root” on UNIX systems) or ask your system administrator for help to complete this task.

Windows 2000/XP

Open the Explorer, navigate to the directory (or share) and press the right mouse button to open the context menu. Select **Sharing** to open the configuration dialog (see Figure 54).

Adjust the settings for the selected directory (see Figure 55).

- Activate the selected directory as a share. Select **Share this folder**.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field **Comment**).
- If necessary, adjust the permissions (button **Permissions**).
- Click **OK** to set the options for this share.

Downloaded from www.Manualslib.com manuals search engine

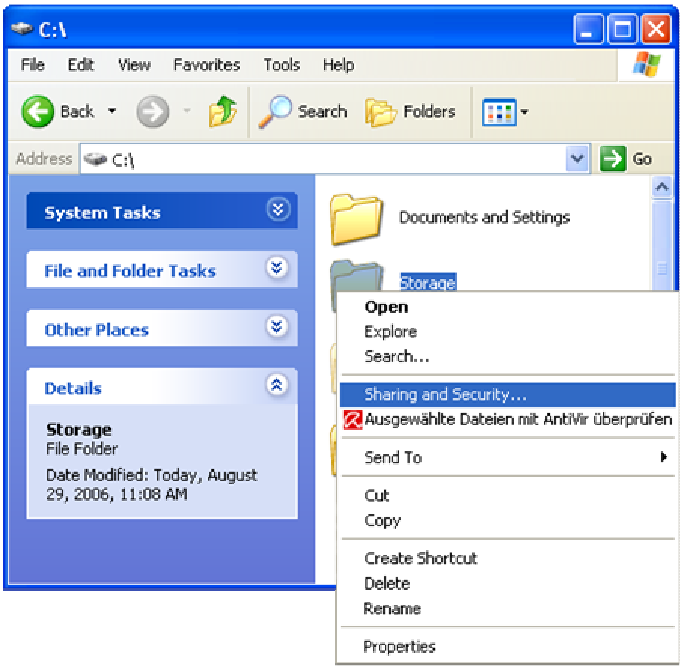


Figure 54 Explorer Context Menu

C:\
File Edit View Favorites Tools Help
Back Search Folders
Address C:\
Go
System Tasks
Storage
File Folder
Storage Properties
General Sharing Security Customize
You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.
Do not share this folder
Share this folder
Share name:
Comment:
User limit:
Maximum allowed
Allow this number of users:
To set permissions for users who access this folder over the network, click Permissions.
Permissions
To configure settings for offline access, click Caching.
Caching
Windows Firewall will be configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

Figure 55 Share Configuration Dialog

Downloaded from www.Manualslib.com manuals search engine

UNIX and UNIX-like OS (UNIX, Solaris, Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file `/etc/samba/smb.conf` or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

For additional options see the **Section: Options** for details.

Drive Redirection

The Drive Redirection is another possibility to use a virtual disc drive on the remote computer. With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that for the remote machine it is possible to write data to your local disc.

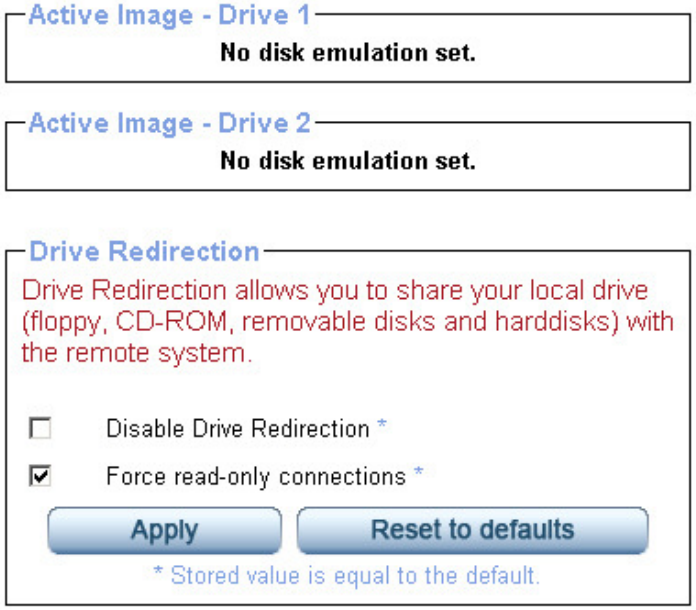

Active Image - Drive 1
No disk emulation set.
Active Image - Drive 2
No disk emulation set.
Drive Redirection
Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.
Disable Drive Redirection *
Force read-only connections *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 56 Drive Redirection

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host's operating system. We recommend to use the Drive Redirection with care, especially the write support.

Drive Redirection Options

As shown in Figure 56 the following options may be enabled:

Downloaded from www.Manualslib.com manuals search engine

Disable Drive Redirection

If enabled the Drive Redirection is switched off.

Force read-only connections

If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

Click **Apply** to submit your changes.

Software Requirements

To use this feature, you have to install the Drive Redirection software that is currently only available for Microsoft Windows. This software can be found on your ARMC/3P CD.

Configuration

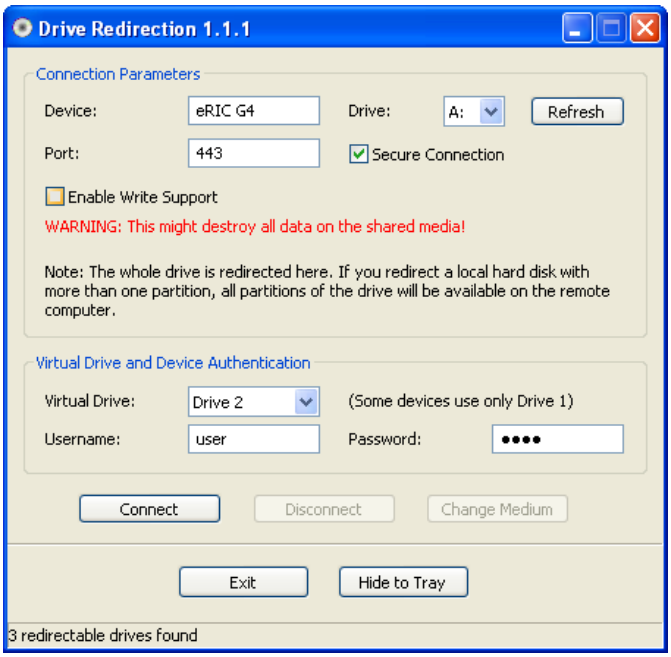


Figure 57 Main View

Specify the parameters of the network connection (see Figure 57).

Device

This is the address (either the DNS name or the IP address) of the ARMC/3P you would like to connect to.

Port

This is the network port. By default, ARMC/3P uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your ARMC/3P's network settings.

Downloaded from www.Manualslib.com manuals search engine

Secure Connection

Enable this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

Drive Selection

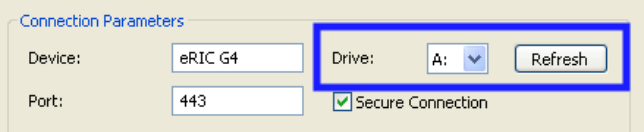


Figure 58 Selecting the desired Drive

Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected.

The **Refresh** button may be used to regenerate the list of drive letters, especially for an USB stick.

Write Support

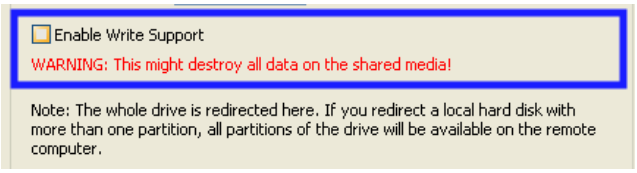

Enable Write Support
WARNING: This might destroy all data on the shared media!
Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Figure 59 Selection Write Support

This feature may be enabled here. Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

Virtual Drive and Device Authentification

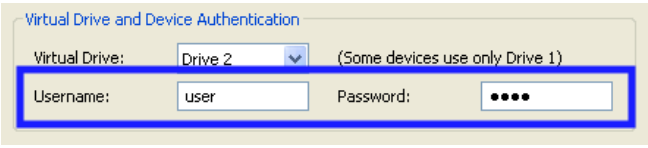


Figure 60 Device Authentification

To use the Drive Redirection, you have to authenticate on the ARMC/3P using a valid username and password. A permission to change the virtual disc configuration is necessary .

With the offered Double Virtual Media feature of the ARMC/3P you have to select the drive you want to use.

Downloaded from www.Manualslib.com manuals search engine

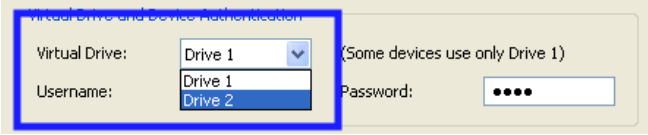


Figure 61 Virtual Drive Selection

Navigation Buttons

Connect/Disconnect

To establish the drive redirection press the **Connect** button once. If all the settings are correct, the status bar displays that the connection has been established, the **Connect** button is disabled and the **Disconnect** button is enabled.

On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

With the Disconnect button, a connection via Drive Redirection connection is stopped.

Exit/Hide

If the **Exit** button is pressed, the Drive Redirection software is closed. If a Drive Redirection connection is active, the connection will be closed before the application terminates.

Using the **Hide to Tray** button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu (see Figure 62).

Figure 62 Tray Info

Options

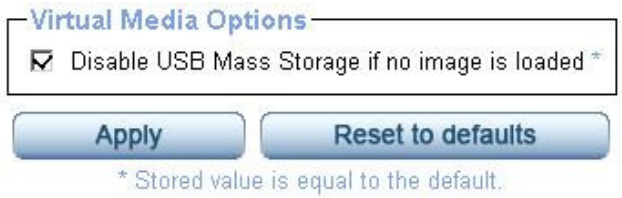

Virtual Media Options
Disable USB Mass Storage if no image is loaded *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 63 USB Mass Storage Option

Downloaded from www.Manualslib.com manuals search engine

Set this option to disable the mass storage emulation (and hide the virtual drive) as long as no image file is currently loaded. If unset and no file image will be found, it may happen that the host system will hang on boot due to changes in the boot order or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS may not be fully excluded. This behaviour depends on the BIOS version used in that machine.

To set this option press the **Apply** button.

Creating an Image

Floppy Images

UNIX and UNIX-like OS

To create an image file make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a floppy image file copy the contents of a floppy to a file. You can use the following command:

dd [`if=/dev/fd0` **][** `of=/tmp/floppy.image` **]**

dd reads the entire disc from the device /dev/fd0 and saves the output in the spec- ified output file `/tmp/floppy.image`. Adjust both parameters exactly to your needs (input device etc.)

MS Windows

You can use the tool “RawWrite for Windows”.

Select the tab **Read** from the menu. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the **Copy** button to initiate the image creation process. For related tools you may have a look at the homepage of the fdos project (`http://www.fdos.org/ripcord/rawrite/`).

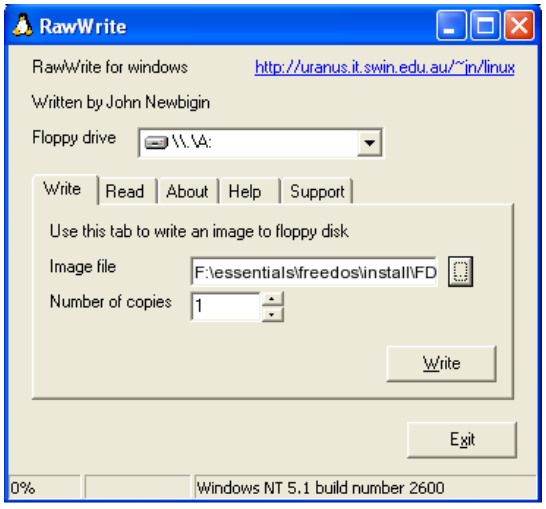


Figure 64 RawWrite for Windows Selection Dialog

Downloaded from www.Manualslib.com manuals search engine

CD ROM/ISO 9660 Images

UNIX and UNIX-like OS

To create an image file make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a CDROM image file copy the contents of the CDROM to a file. You can use the following command:

dd [`if=/dev/cdrom` **] [** `of=/tmp/cdrom.image` **]**

dd reads the entire disc from the device `/dev/cdrom` and saves the output in the specified output file `/tmp/cdrom.image`. Adjust both parameters exactly to your needs (input device etc.).

MS Windows

To create the image file use your favourite CD imaging tool. Copy the whole contents of the disc into one single ISO image file on your harddisk. For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the **Copy Disc** section. Select the CD ROM or DVD drive you would like to create an ISO image from. Specify the filename of the ISO image and save the CD ROM content in that file.

Figure 65 Nero Selection Dialog

Downloaded from www.Manualslib.com manuals search engine

System Health

The IPMI support on the host system enables you to power on or off the host system or to perform a hard reset over the ARMC/3P. Furthermore, it provides the possibility to show an event log of the host system and the status of some system sensors (i.e. temperature).

Chassis Control

With Chassis Control one can

- Get the information of the specified chassis
- Switch host power on/off
- Locate host chassis
- Enable/disable the Power, Reset, NMI buttons on the front panel

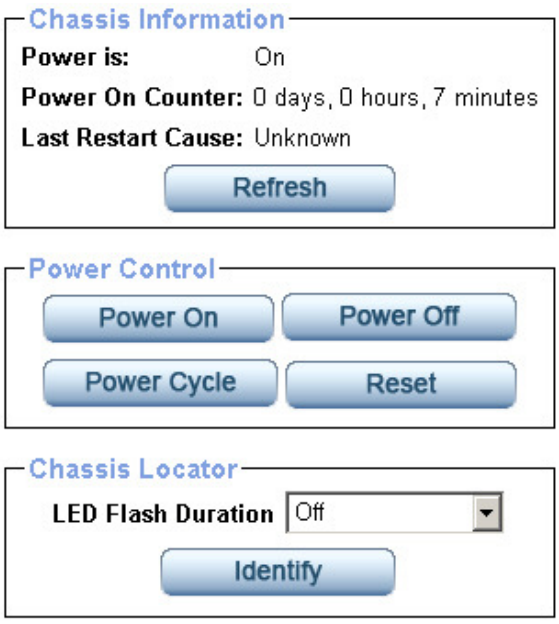


Figure 66 Chassis Control

Monitor Sensors

Some of the sensors on the host will be listed here.

Downloaded from www.Manualslib.com manuals search engine

Monitoring Sensors

Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Temperature	CPU 1 Temp 1	Ok	31 degrees C
Temperature	CPU 1 Temp 2	No reading	
Temperature	CPU 2 Temp 1	No reading	
Temperature	CPU 2 Temp 2	No reading	
Temperature	SYS Temp	Ok	41 degrees C
Temperature	BP1_Temp	Ok	28 degrees C
Temperature	BP2_Temp	Ok	29 degrees C
Voltage	P_VCCP0	Ok	1.288 Volts
Voltage	P_VCCP1	No reading	

Figure 67 Monitor Sensors Overview

System Event Log

You can browse the System event logs here. Please note that these logs are for IPMI events, they are independent to the system logs of the OPMA add-on card.

System Event Log

Event Type	Date	Time	Source	Description	Direction
SEL record 02	05/06/2006	00:58:34	CPU 2 Temp 2		Assertion Event
SEL record 02	Pre-Init	00:06:00	NMI	OEM System boot event	Assertion Event
SEL record 00	Pre-Init	00:05:50	System ACPI Power State	S0/G0: working	Assertion Event
SEL record 02	Pre-Init	00:00:06	A/C Lost	AC lost	Assertion Event
SEL record 02	Pre-Init	00:00:06	A/C Lost	AC lost	Assertion Event

Figure 68 System Event Log Overview

Alarm Settings

Here you can see all the alerts of the system. You can also define the filters, policies and LAN destinations, to which the alerts will be sent. For more details please consult the IPMI specifications.

IPMI Alert Configuration

[Filter List] [Policy List] [LAN Destination List]

IPMI Filter List

Index	Status	Filter Type	Action	Policy#	Severity	Generator ID		Sensor Type	Sensor No	Trigger	Offset Mask	Data 1			Data 2			Data 3			
1	enabled	predefined	alert poweroff reset power cycle	1	non-recoverable	ff	ff	04	ff	01	3000	fe	ff	54	00	ff	00	00	ff	00	[edit]
2	enabled	predefined	alert poweroff reset power cycle	1	critical	ff	ff	04	ff	01	0c00	fe	ff	52	00	ff	00	00	ff	00	[edit]
3	enabled	predefined	alert	1	non-critical	ff	ff	04	ff	01	0300	fe	ff	50	00	ff	00	00	ff	00	[edit]
4	enabled	predefined	alert	1	non-critical	ff	ff	04	ff	01	c000	fe	ff	56	00	ff	00	00	ff	00	[edit]
5	enabled	predefined	alert	1	critical	ff	ff	04	ff	01	0003	fe	ff	58	00	ff	00	00	ff	00	[edit]

Figure 69 IPMI Alarm Configuration

Downloaded from www.Manualslib.com manuals search engine

User Management

Change Password

Figure 70 Set Password

To change your password enter the new password in the upper entry field. Retype the password in the field below.

Click **Apply** to submit your changes.

User and Groups

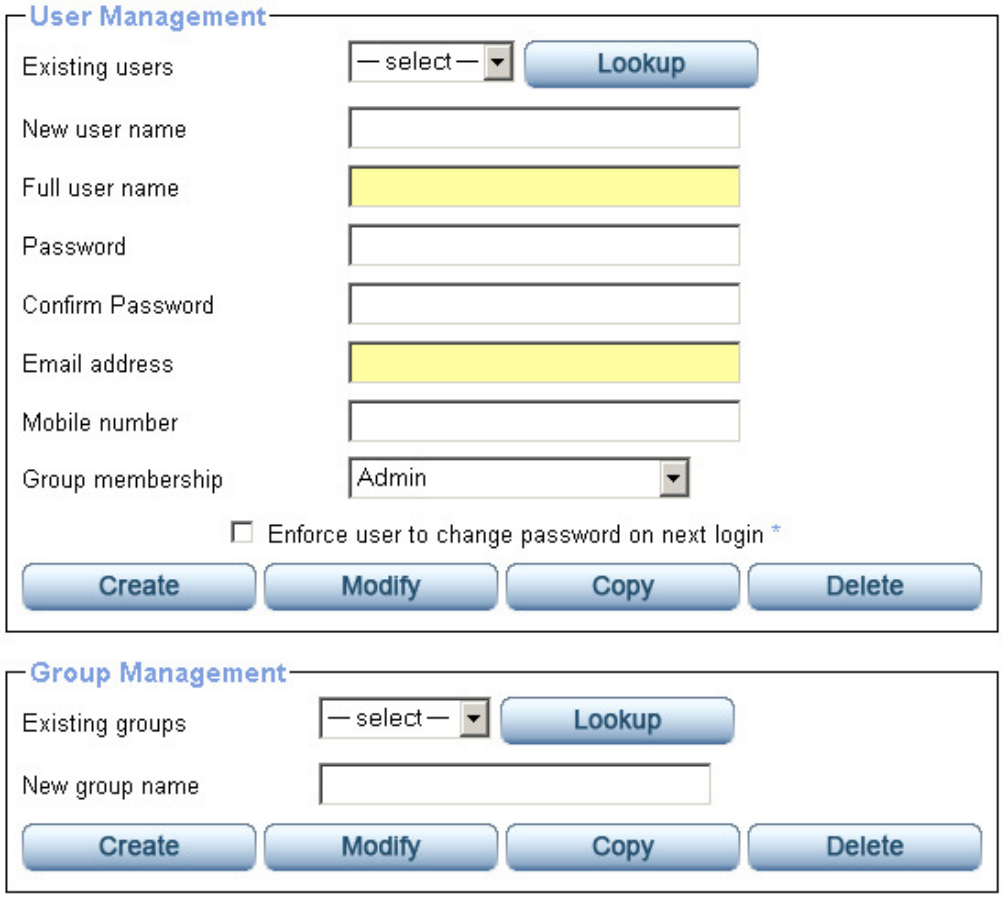


Figure 71 User/Group Management

Downloaded from www.Manualslib.com manuals search engine

User Management

The configurable settings of the ARMC/3P are split into user settings (basically authentication and user information) and group settings (authorization).

There is one predefined user "admin" and two predefined group "admin" and "<unknown>", which cannot be renamed or deleted.

Each user may be member of one group and inherits permissions set for this group. If a user is not member of a group, permissions can be set exclusively for that user. The user “admin” is always member of admin group which has full system access. The <unknown> group initially does not have any permissions, but is modifiable.

Users can authenticate against a remote authentication service (such as LDAP or RADIUS). If this remote authentication service returns an invalid or no group assignment, the user is considered to be member of the <unknown> group.

Upon delivery, the account for the user “admin” has the password “password”. Make sure to change the password immediately after you have installed and first accessed your ARMC/3P.

A full list of available options follows. This list can only be seen by the admin.

Existing users

Select an existing user for modification. Once a user has been selected, click the **Lookup** button to see the user information.

New User name

The new user name for the selected account.

Password

The password for the login name. It must be at least four characters long.

Confirm password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

Dial-back number

This information may be optionally provided.

Downloaded from www.Manualslib.com manuals search engine

Existing groups

Select an existing group for modification. Each user can be a member of a group - either an administrator or a regular user. Choose the desired group from the selection box.

New group name

The new group name for the selected account.

To create a user or a group press the **Create** button. The **Modify** button changes the displayed user settings. To delete an user or group press the **Delete** button.

Note: The ARMC/3P is equipped with an host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not to exceed the number of 25 users connected to the ARMC/3P at the same time. The memory space that is available onto the ARMC/3P mainly depends on the configuration and the usage of the ARMC/3P (log file entries etc.). That's why we recommend not to store more than 150 group profiles.

Permissions

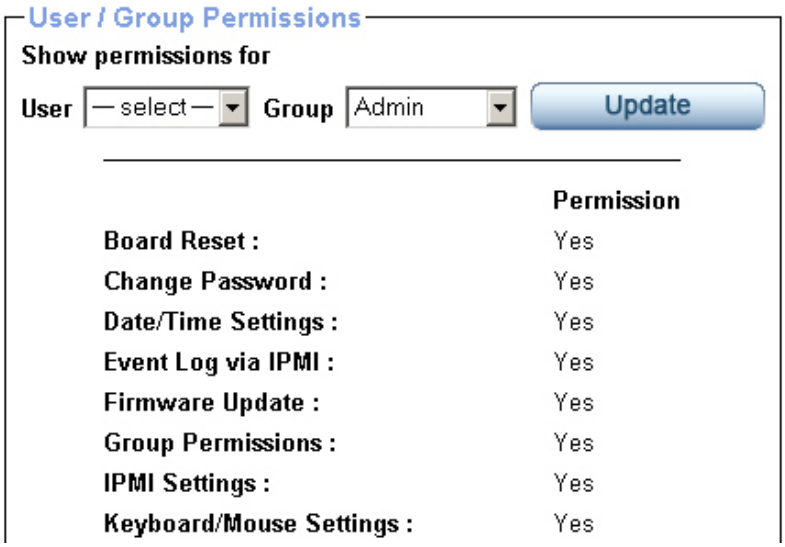


Figure 72 User/Group Permission Settings

Here you can define the permissions for the different groups. All users of one group will have the same rights. When you want to change the permissions for one special user you have to define a new group for him.

Downloaded from www.Manualslib.com manuals search engine

KVM Settings

User Console

The following settings are user specific. That means the admin can customize these settings for every user separately. Changing the settings for one user does not affect the settings for the other users.

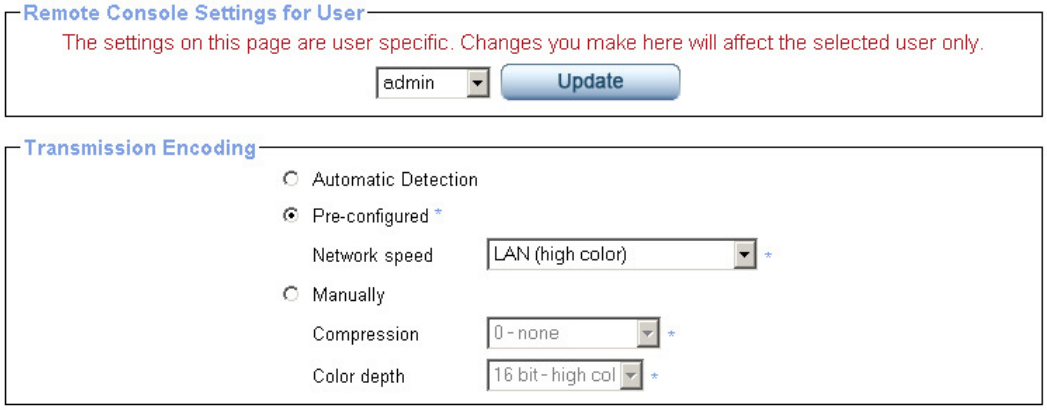


Figure 73 User Console Settings (Part 1)

Remote Console Settings for User

This selection box displays the user ID for which the values are shown and for which the changes will take effect. Select the desired user from the selection box and press the **Update** button. This will result in displaying the according user settings below.

Note: You are allowed to change the settings of other users only if you have the necessary access rights for this task. For a regular user without the correct permissions it is not possible to change the settings for any other users.

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and color depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the color depth individually.

Downloaded from www.Manualslib.com manuals search engine

Depending on the selected compression rate the data stream between the ARMC/3P and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used while several users are accessing the ARMC/3P simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

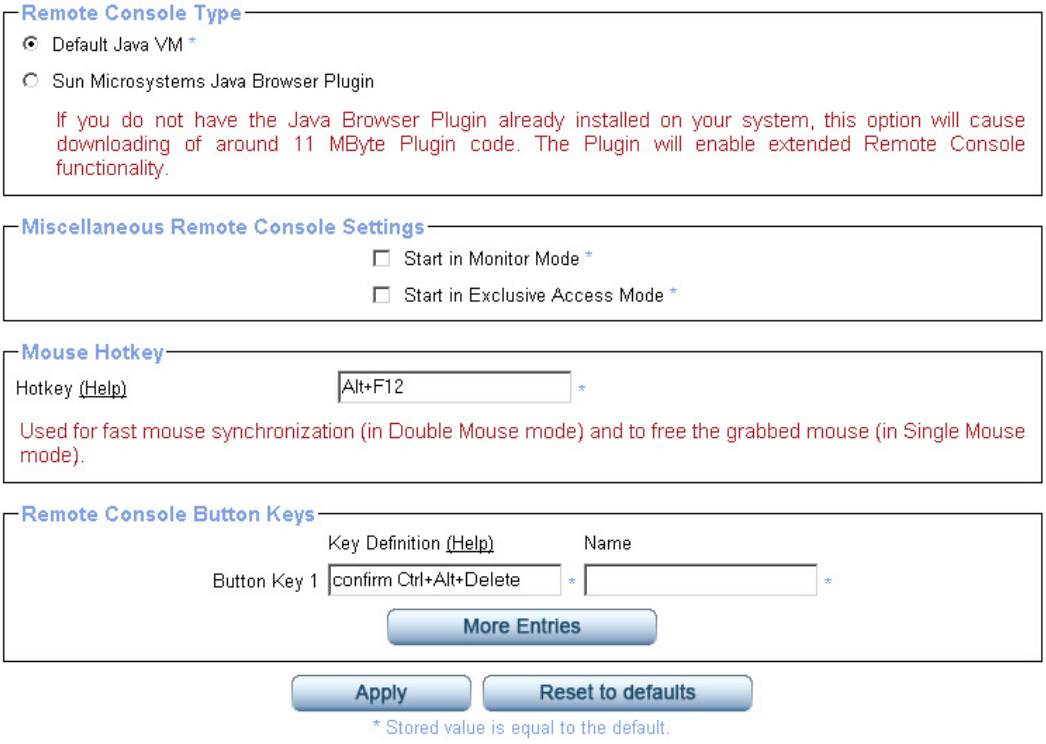

Remote Console Type
Default Java VM *
Sun Microsystems Java Browser Plugin
If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.
Miscellaneous Remote Console Settings
Start in Monitor Mode *
Start in Exclusive Access Mode *
Mouse Hotkey
Hotkey (Help)
Alt+F12 *
Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).
Remote Console Button Keys
Key Definition (Help)
Name
Button Key 1
confirm Ctrl+Alt+Delete *
*
More Entries
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 74 User Console Settings (Part 2)

Specifies which Remote Console Viewer to use.

Default Java Virtual Machine (JVM)

Uses the default JVM of your web browser. This may be the Microsoft JVM for the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java

Downloaded from www.Manualslib.com manuals search engine

plug-in is not yet installed on your system, it may be downloaded and installed automatically. However, in order to make the installation possible, you still have to answer the according dialogs with “yes”. The download volume is around 11 Mbytes. The advantage of downloading Sun’s JVM is the usage of a stable and identical JVM across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in SUN’s JVM.

Important: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine.

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is disabled. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. Nobody else can open the Remote Console at the same time again until you disable this feature or log off.

Mouse Hotkey

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or just the fact that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are “Control+Alt+Delete” on Windows and DOS, that is always caught, or the key sequence “Control+Backspace” on Linux that can be used for terminating the X-Server.

In order to define a new Button Key or to adjust an existing one have a look at the rules that describe the setting for a key. In general, the syntax for a key is as follows:

[confirm] <keycode>[+|-|<[*]<keycode>]*

A term in brackets is optional. The star at the end means that you add further keys as often as required for your case. The term “confirm” adds an confirmation dialogue that is displayed before the key strokes will be sent to the remote host.

The “keycode” is the key to be sent. Multiple key codes can be concatenated with either a plus, a minus, or an “<” sign. The plus sign builds key combinations - all

Downloaded from www.Manualslib.com manuals search engine

the keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So, the minus sign builds single, separate keypresses and keyreleases. The “<” sign releases the last key, only. The star inserts a pause with a duration of 100 milliseconds.

As an example, the key combination of Ctrl, Alt and F2 is represented by the sequence

Ctrl+Alt+F2

For a full list of key codes and aliases please refer to the **Appendix C:** Key Codes.

Key Definition

Enter your desired key combination as described above.

Name

You may also name your button that will be visible in the Remote Console Control Bar. If unspecified the sequence of keys will be displayed, instead.

> ***Note***
>
> If you need more button keys than shown use the **more entries** button. This will open a list of additional entry fields.

Power Control

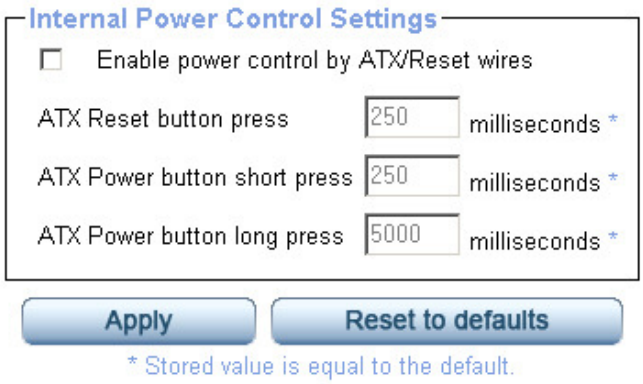


Figure 75 Power Control

The Power Control panel enables the access to the most important external buttons of your host system besides from the keyboard. These buttons are the reset and the power button. To enable power control by ATX/Reset wires, set this option. Furthermore, the duration the according button is pressed can be adjusted.

Set the duration for

- ATX Reset button press
- ATX Power button short press
- ATX Power button long press

Downloaded from www.Manualslib.com manuals search engine

Then, click **Apply** to submit your changes.

Keyboard/Mouse

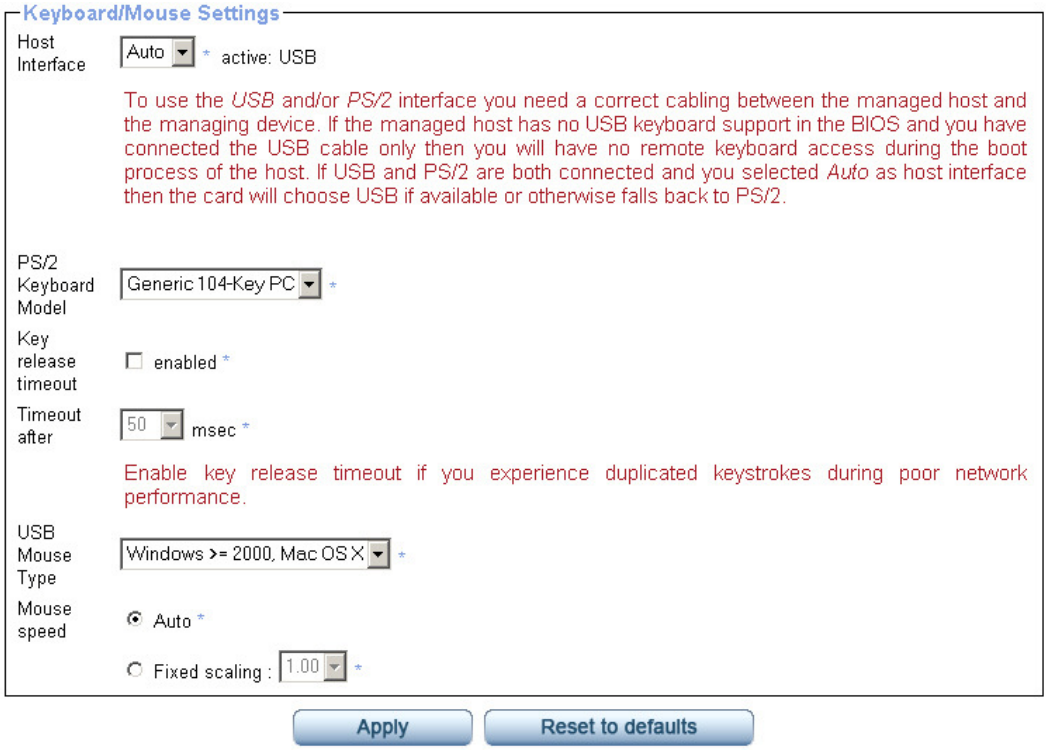

Keyboard/Mouse Settings
Host Interface
Auto
active: USB
To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected Auto as host interface then the card will choose USB if available or otherwise falls back to PS/2.
PS/2 Keyboard Model
Generic 104-Key PC
Key release timeout
enabled
Timeout after
50
msec
Enable key release timeout if you experience duplicated keystrokes during poor network performance.
USB Mouse Type
Windows >= 2000, Mac OS X
Mouse speed
Auto
Fixed scaling :
1.00
Apply
Reset to defaults

Figure 76 Keyboard and Mouse Settings

Host Interface

Enables a certain interface the mouse is connected to. You can choose between **Auto** for automatic detection, **USB** for a USB mouse and **PS/2** for a PS/2 mouse.

Important: To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected "Auto" as host interface, then the card will select "USB" if available or otherwise falls back to "PS/2".

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- the host BIOS must have USB keyboard support
- the USB cable must be connected or must be selected in the Host interface option

Downloaded from www.Manualslib.com manuals search engine

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extended by three additional Windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for the Apple Macintosh.

If a keyboard timout is required the according option can be enabled. Additionally, set the desired time value in the input field below.

USB Mouse Type

Enables the USB mouse type. Choose an appropriate option from the selection box. For a detailed description about the mouse type and recommended options for the different operating systems see the Section: Recommended Mouse Settings in Chapter 3.

Mouse Speed

Auto mouse speed

Use this option if the mouse settings on the host use an additional acceleration setting. The ARMC/3P tries to detect the acceleration and speed of the mouse during the mouse sync process.

Fixed mouse speed

Use a direct translation of mouse movements between the local and the remote pointer.

You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

To set the options click **Apply**.

Video

Host Monitor Settings

Using this option (see Figure 77) it is possible to add video modes to the ARMC/3P which are not recognized using the factory settings. This may be useful when using special modelines in a X-Window configuration on the host or with uncommon hosts or operating systems. From the selection box you may choose the desired screen resolution for the local monitor.

Important: This option is for advanced users only. It is possible to influence the correct video transmission by using this option. We recommend to use with care.

The maximum number of the custom video resolution is 4. Using the option **Custom Modes Handling** custom modes may be either disabled (Off), additionally used to

Downloaded from www.Manualslib.com manuals search engine

the standard video resolution or used in an exclusive way (Only). With the last option it is also possible to force a special video mode for the ARMC/3P. To change the parameters for a certain video mode choose the according number from the selection box and press the **Update** button. It is necessary to provide some additional information so that the video mode may be correctly recognized:

X Resolution
Visible number of horizontal pixels.

Y Resolution
Visible number of vertical pixels.

Horizontal Frequency (Hz)
The horizontal (line) frequency in Hz.

Vertical Frequency (Hz)
The vertical (refresh) frequency in Hz.

Total horizontal pixels
The total amount of pixels per line, including the non-visible and blanking area.

Polarity
The polarity (positive/negative) of the synchronization signals. V means vertical, H means horizontal polarity.

Description
Here you can provide a mode name which is displayed in the Remote Console if this custom mode is activated.

Downloaded from www.Manualslib.com manuals search engine

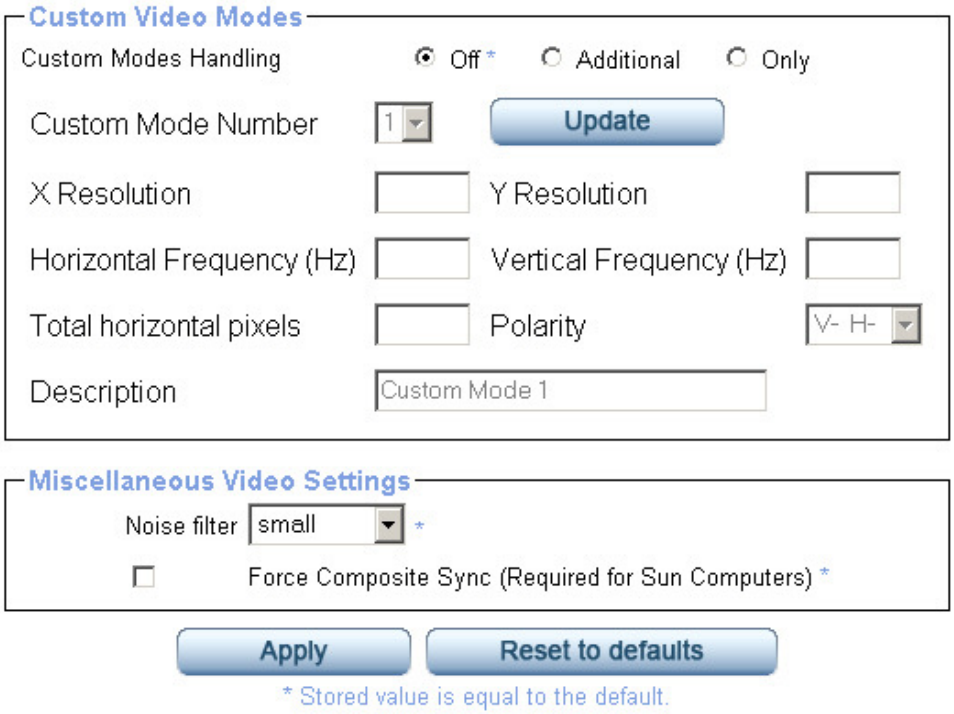


Figure 77 Video Settings

To set the options (see below) click on the **Apply** button.

Miscellaneous Video Settings

Noise filter

This option defines how the ARMC/3P reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a con- stant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Force Composite Sync (Required for Sun Computers)

To support signal transmission from a Sun machine enable this option. If not enabled the picture of the remote console will not be visible.

Downloaded from www.Manualslib.com manuals search engine

Device Settings

Network

The **Network Settings** panel as shown in Figure 78 allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

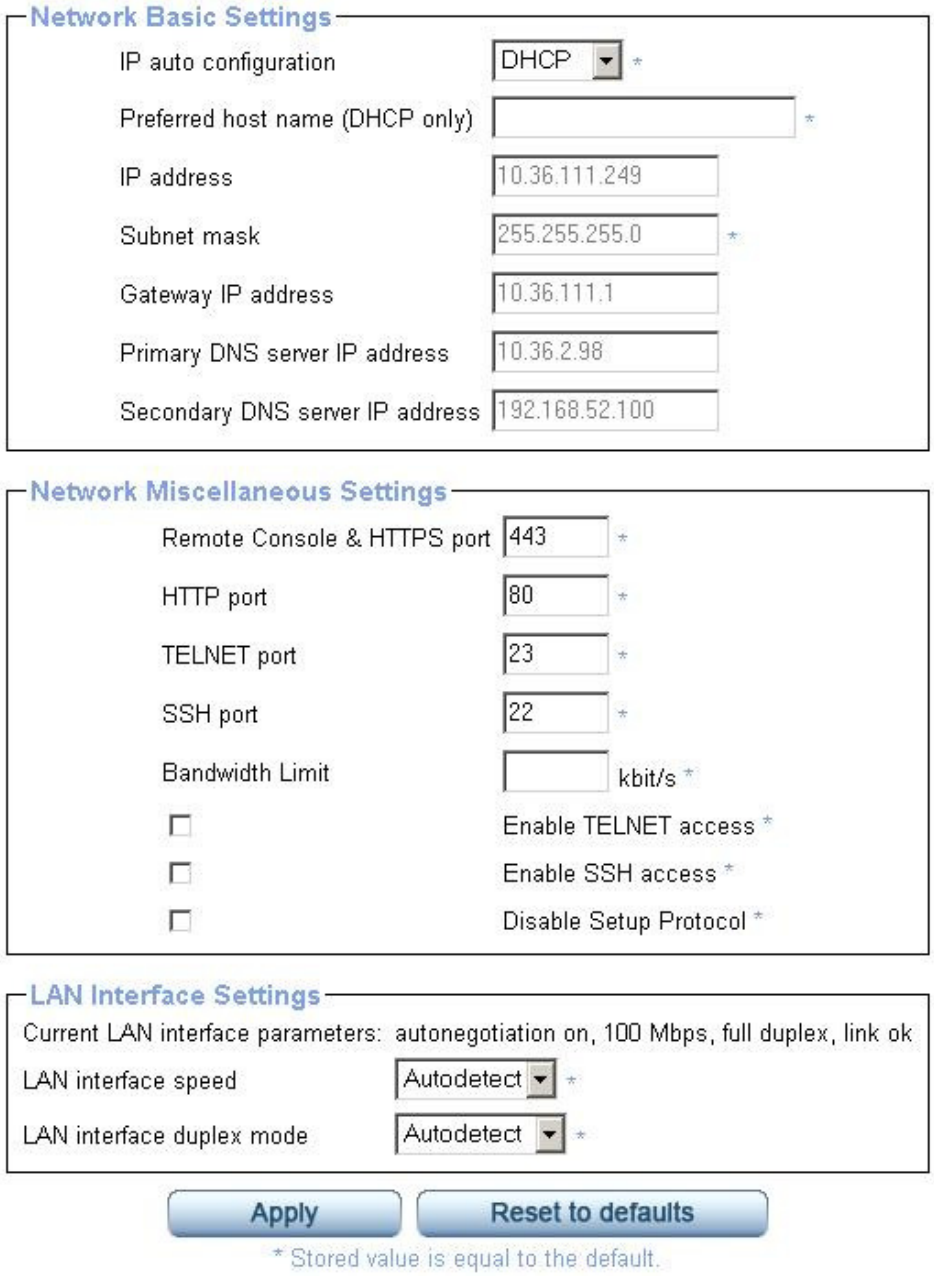


Figure 78 Network Settings

Important: The initial IP configuration is usually done directly at the host system using the special procedure described in Table 4 Initial Network Configuration.

Downloaded from www.Manualslib.com manuals search engine

Important: Changing the network settings of the ARMC/3P might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the ARMC/3P.

Basic Network Settings

IP auto configuration

With this option you can define if the ARMC/3P should fetch its network settings from a DHCP or BOOTP server. For DHCP select “dhcp” and for BOOTP select “bootp” accordingly. If you choose “none” then IP auto configuration is disabled.

Preferred host name

Preferred host name to request from DHCP server. Whether the DHCP server takes the ARMC/3P’s suggestion into account or not depends on the server configuration.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the ARMC/3P should be accessible from networks other than the local one, this IP address must be set to the local network router ’s IP address.

Primary DNS Server IP Address

IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the ARMC/3P will not be able to perform name resolution.

Secondary DNS Server IP Address

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Miscellaneous Network Settings

Remote Console And HTTPS port

Port number at which the ARMC/3P’s Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port

Port number at which the ARMC/3P’s HTTP server is listening. If left empty the default value will be used.

Downloaded from www.Manualslib.com manuals search engine

Telnet port

Port number at which the ARMC/3P's Telnet server is listening. If left empty the default value will be used.

SSH port

Port number at which the ARMC/3P's Secure Shell (SSH) server is listening. If left empty the default value will be used.

Bandwidth Limit

The maximum network traffic generated through the ARMC/3P Ethernet device. Value in Kbit/s.

Enable Telnet access

Set this option to allow accessing the ARMC/3P using the Telnet gateway (see the **Chapter 5: Telnet Console**).

Enable SSH access

Set this option to allow accessing the ARMC/3P using the Secure Shell (SSH) protocol. This SSH console offers the same features as Telnet (see the **Chapter 5: Telnet Console**), but uses a secure, encrypted connection instead.

Disable Setup Protocol

Enable this option to exclude the ARMC/3P from the setup protocol.

LAN Interface Settings

This entry field displays the current settings for the Ethernet/LAN interface of the ARMC/3P. You may choose between auto negotiation and a fixed setting for the Ethernet transceiver settings "interface speed" and "duplex mode" in case auto negotiation does not work correctly.

LAN interface speed

Depending on your network connection you may select an according speed value for this interface. To adjust the interface automatically choose "autodetect" (default value). If this selection results in misbehavior of the interface, choose one of other speed options to work with. The interface will transmit and receive data with that fixed speed.

LAN interface duplex mode

If necessary you may also select a specific duplex mode. The default value is set to "autodetect" which leads to an automatic setting of the duplex mode depend- ing on your network (recommended). As an alternative you may explicitly set the interface to either "half duplex" or "full duplex" mode.

These settings may also be configured via serial console. See **Chapter 3: Initial Configuration via Serial Console** for details.

Downloaded from www.Manualslib.com manuals search engine

Dynamic DNS

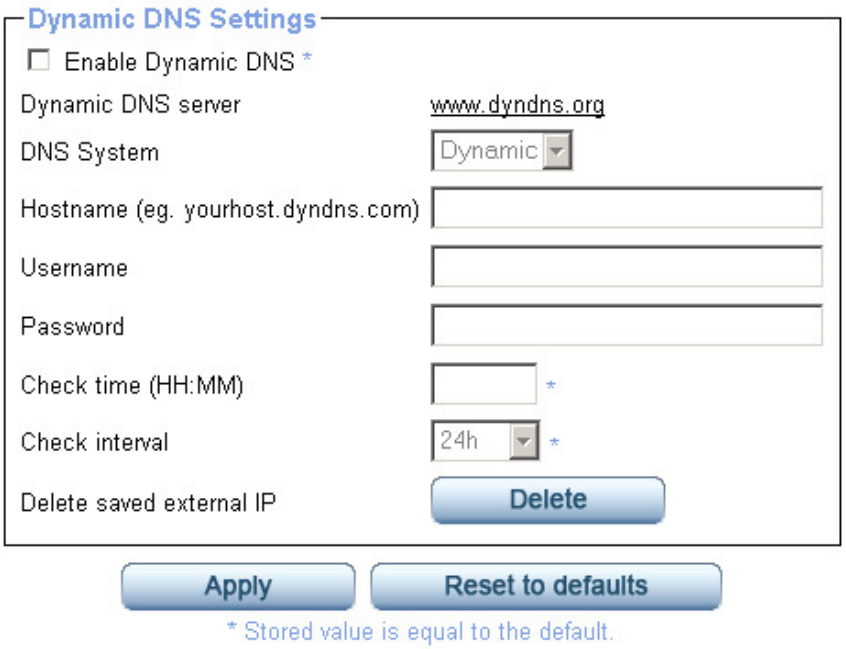


Figure 79 Dynamic DNS

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario (see Figure 80 Dynamic DNS Scenario):

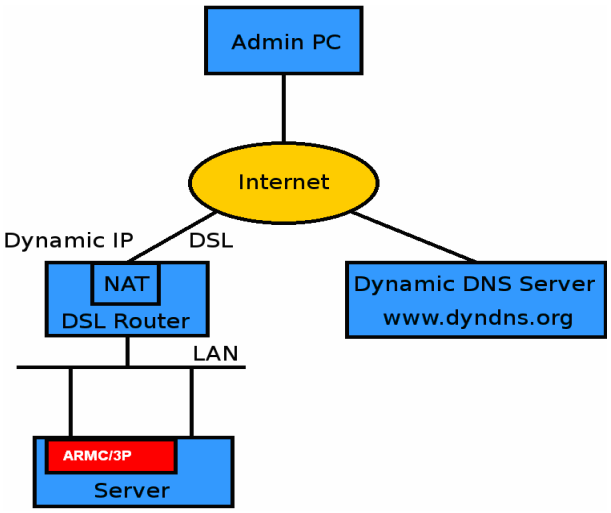


Figure 80 Dynamic DNS Scenario

Downloaded from www.Manualslib.com manuals search engine

The ARMC/3P is reachable via the IP address of the DSL router which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the ARMC/3P connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to the card.

The administrator has to register an ARMC/3P that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return from the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered ARMC/3P.

You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the ARMC/3P is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure 79.
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server

This is the server name where ARMC/3P registers itself in regular intervals. Currently this is a fixed setting since only dyndns.org is supported for now.

Hostname

This is the hostname of the ARMC/3P that is provided by the Dynamic DNS Server (use the whole name including the domain, e.g. testserver.dyndns.org, not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The ARMC/3P card registers itself in the Dynamic DNS server at this time.

Check interval

This is the interval for reporting again to the Dynamic DNS server by the ARMC/3P.

Important: The ARMC/3P has its own independent real time clock. Make sure the time setting of the ARMC/3P is correct (see Chapter 5: Date/Time).

Downloaded from www.Manualslib.com manuals search engine

Security

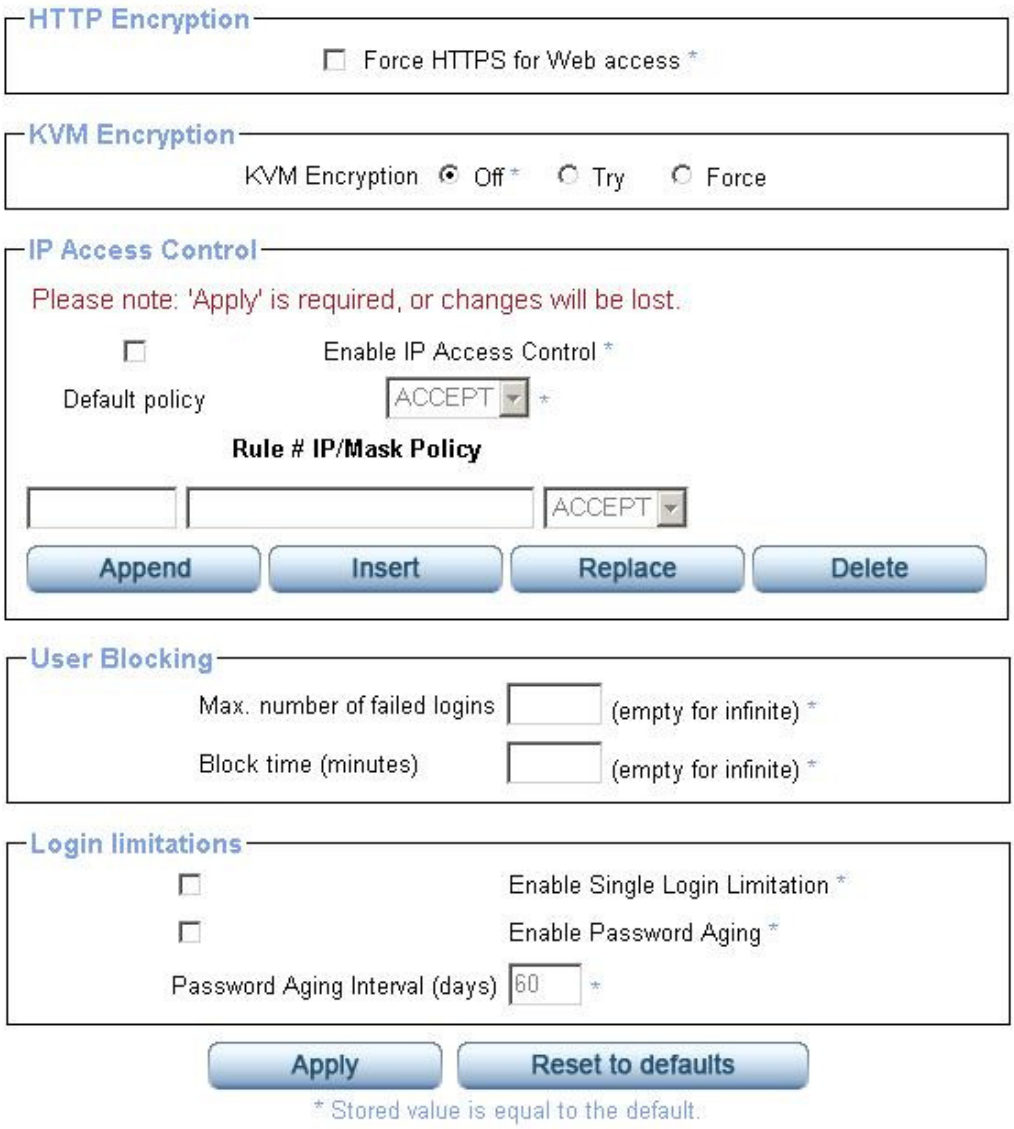


Figure 81 Security Settings

Encryption Settings

Force HTTPS

If this option is enabled, access to the web front-end is only possible using a HTTPS connection. The ARMC/3P will not listen on the HTTP port for incoming connections.

In case you want to create your own SSL certificate that is used to identify the ARMC/3P, refer to **Chapter 5: Certificate**.

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the

Downloaded from www.Manualslib.com manuals search engine

Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host.

If set to **Off** no encryption will be used. If set to **Try** the applet tries to make an encrypted connection. If the connection cannot be established an unencrypted connection will be used instead. If set to **Force** the applet tries to make an encrypted connection. An error will be reported in case the connection establishment fails.

IP Access Control

This section explains the settings related to IP access control. It is used to limit the access to a distinguished number of clients only. These clients will be identified by their IP address from which they are trying to build up a connection.

Important: The IP access control settings apply to the LAN interface only!

Enable IP Access Control

Enables access control based on IP source addresses.

Default policy

This option controls what to do with arriving IP packets that do not match any of the configured rules. They can be accepted or dropped.

Important: If you set this to "DROP" and you have no "ACCEPT" rules configured, the access to the web front end over LAN is actually impossible! To enable access again you can change the security settings via modem or by temporarily disabling IP access control with the initial configuration procedure (see Table 4).

Rule Number

This should contain the number of a rule for which the following commands will apply. In case of appending a new rule, this field will be ignored.

IP/Mask

Specifies the IP address or IP address range for which the rule applies. Examples (the number concatenated to an IP address with a "/" is the number of valid bits that will be used of the given IP address):

`192.168.1.22/32`	Matches the IP Address 192.168.1.22
`192.168.1.0/24`	Matches all IP packets with sources addresses from 192.168.1.0 to 192.168.1.255
`0.0.0.0/0`	Matches any IP packet

Downloaded from www.Manualslib.com manuals search engine

Policy

The policy determines what to do with matching packets. They can be either accepted or dropped.

Important: The order of the rules is important. The rules are checked in ascending order until a rule matches. All the rules below the matching one will be ignored. The default policy applies if no match has been found.

Appending a rule

Enter the IP/Mask and set the policy. Finally, press the **Append** button.

Inserting a rule

Enter the rule number, the IP/Mask and set the policy. Finally, press the **Insert** button.

Replacing a rule

Enter the rule number, the IP/Mask and set the policy. Finally, press the **Replace** button.

Deleting a rule

Enter the rule number and press the **Delete** button.

Anti Brute Force Setting

The Anti Brute Force user blocking mechanism allows to disable the login of a certain user if his password was entered incorrectly for a specific number of times. The duration of the blocking is also configurable.

Maximum number of failed logins

Enter the maximum number of failed login attempts after which it should not be possible for this user to login anymore. Leave this field empty to disable the user blocking feature.

Block time

The number of minutes the user is blocked after he exceeded his maximum number of failed login attempts. Leave this field empty to block him for an infinite amount of time until he is manually unblocked again.

Unblocking Users

There are two possibilties to unblock a blocked user.

- A parent user may go to the user management settings (see **User Management)** and press the **Unblock** button for the user.
- It is also possible to use the serial console for the initial configuration (see Table 4) and login as the user “unblock”. The ARMC/3P will ask for the superuser password ans present a list of blocked users which may be unblocked.

Downloaded from www.Manualslib.com manuals search engine

Login Limitations

Single Loging Limitation

If this option is enabled, the user can access the ARMC/3P only from one IP adress with one connection. It is not possible to access the ARMC/3P from different IP addresses or web browsers with the same login at the same time. You have to be logged out or the session has to be timed out to get a new connection on a different IP address on the ARMC/3P with this login.

Password Aging

If this option is enabled after a defined interval a reminder will request a new password for the user. The set interval displays how many days the password is active.

Certificate

The ARMC/3P uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the ARMC/3P has to expose its identity to a client using a cryptographic certificate. Upon delivery this certificate and the underlying secret key is the same for all ARMC/3P ever produced and certainly will not match the network configuration that will be applied to the ARMC/3P cards by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

However, it is possible to generate and install a new base64 x.509 certificate that is unique for a particular ARMC/3P card. In order to do that, the ARMC/3P is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are and signs and issues a SSL certificate to you.

Downloaded from www.Manualslib.com manuals search engine

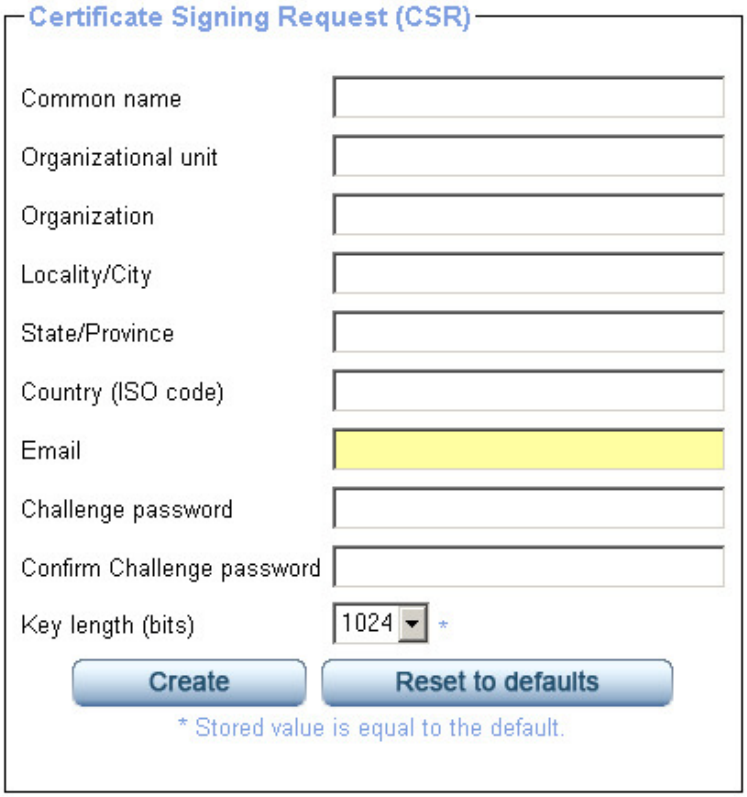


Figure 82 Certificate Settings

To create and install a SSL certificate for the ARMC/3P the following steps are necessary:

- Create a SSL Certificate Signing Request using the panel shown in Figure 82. You need to fill out a number of fields that are explained below. Once this is done, click on the **Create** button which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download** button (see Figure 83).
- Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
- Upload the certificate to the ARMC/3P using the **Upload** button as shown in Figure 83.

Downloaded from www.Manualslib.com manuals search engine

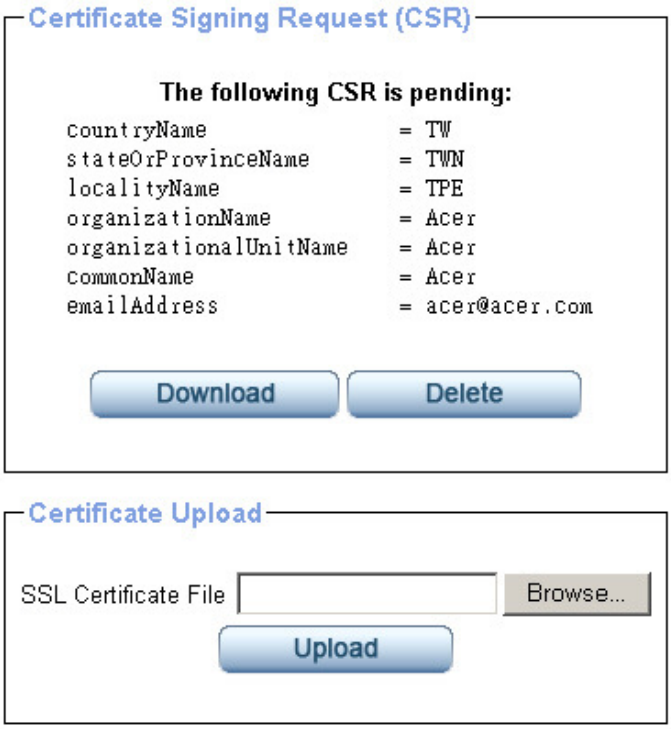


Figure 83 SSL Certificate Upload

After completing these three steps the ARMC/3P has its own certificate that is used for identifying the card to its clients.

Important: If you destroy the CSR on the ARMC/3P there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name

This is the network name of the ARMC/3P once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the ARMC/3P with a web browser but without the prefix "http://". In case the name given here and the actual network name differ, the browser will pop up a security warning when the ARMC/3P is accessed using HTTPS.

Organizational unit

This field is used for specifying to which department within an organization the ARMC/3P belongs.

Organization

The name of the organization to which the ARMC/3P belongs.

Locality/City

The city where the organization is located.

Downloaded from www.Manualslib.com manuals search engine

State/Province
The state or province where the organization is located.

Country (ISO code)
The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.

Challenge Password
Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimum length of this password is four characters.

Confirm Challenge Password
Confirmation of the Challenge Password.

Email
The email address of a contact person that is responsible for the ARMC/3P and its security.

Key length
This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the ARMC/3P during connection establishment.

Serial Port

The ARMC/3P Serial Settings (Figure 84) for Serial Port 1 allow you to specify what device is connected to the serial port and how to use it. With an additional bracket you can use the Serial Port 2 via Telnet/SSH.

Downloaded from www.Manualslib.com manuals search engine

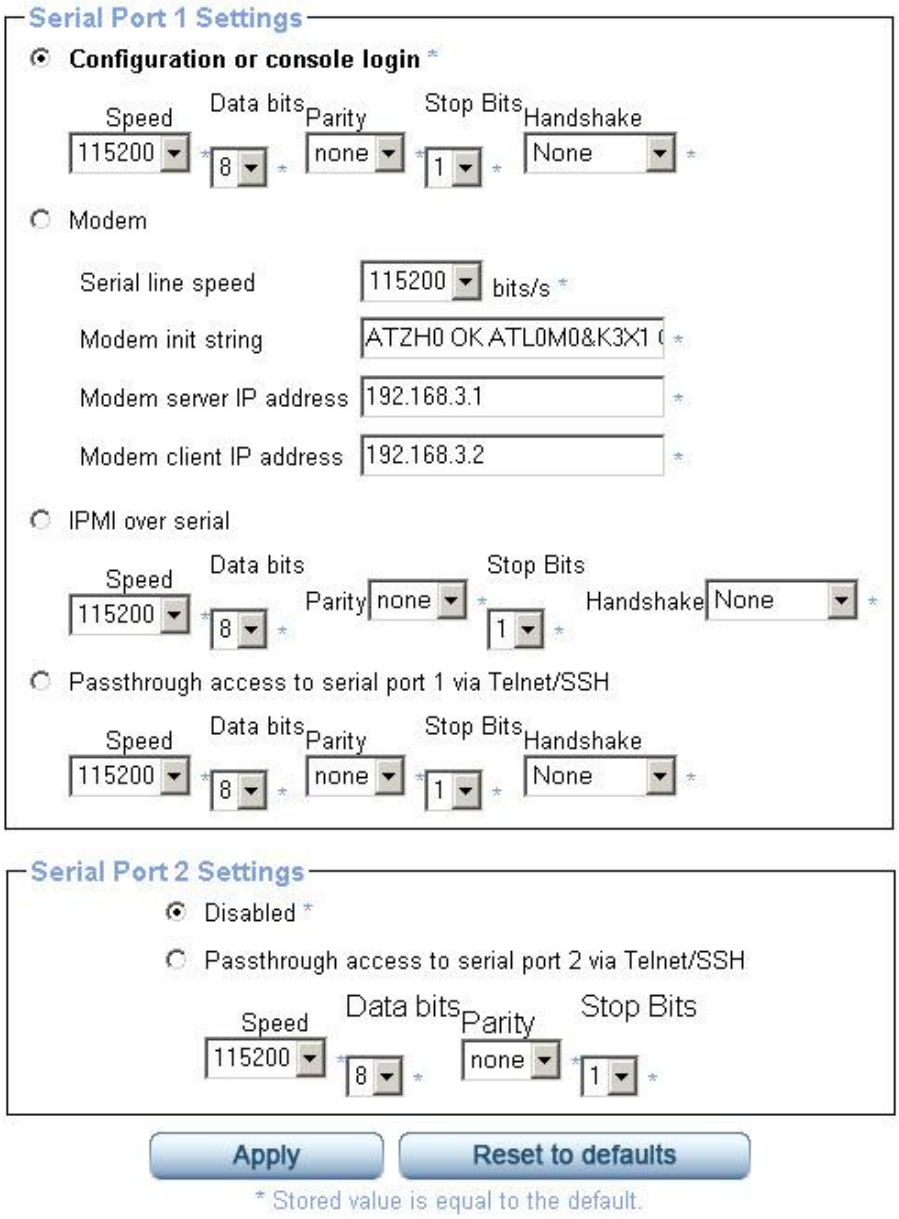


Figure 84 Serial Settings

Configuration or console login

Do not use the serial port for any special function, use it only for the initial configuration (see Table 4 Initial Network Configuration).

Modem

The ARMC/3P offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the ARMC/3P.

Logically, connecting to the ARMC/3P using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the ARMC/3P. In other words, the ARMC/3P acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established

Downloaded from www.Manualslib.com manuals search engine

using the Point-to-Point Protocol (PPP). Before you connect to the ARMC/3P make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection which defaults to the right settings like PPP.

The Modem Settings panel allows you to configure the remote access to the ARMC/3P using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.

Serial line speed

The speed with which the ARMC/3P is communicating with the modem. Most of all modems available today will support the default value of 115,200 bps. In case you are using an old modem and discovering problems try to lower this speed.

Modem Init String

The initialization string used by the ARMC/3P to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.

Modem server IP address

This IP address will be assigned to the ARMC/3P itself during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the ARMC/3P and your console computer. The default value will work in most cases.

Modem client IP address

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the ARMC/3P and your console computer. The default value will work in most cases.

Passthrough access to serial port via Telnet/SSH

Using this option it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet or SSH. Select the appropriate options for the serial port and use the Telnet Console or a standard Telnet/SSH client to connect to the ARMC/3P. For more information about the Telnet interface you may have a look at the **Chapter 5: Remote Console, Telnet Console**.

Downloaded from www.Manualslib.com manuals search engine

Intelligent Platform Management Interface (IPMI)

Generals

By using the ARMC/3P IPMI facilities you have an additional way to power on or off the system or to perform a hard reset. Furthermore, it provides the possibility to show an event log of the host system and the status of some system sensors (i.e. temperature). If your host system supports IPMI, you can access it by one of the following ways:

- IPMI over IPMB
- IPMI over LAN (IPMI V1.5 is required)

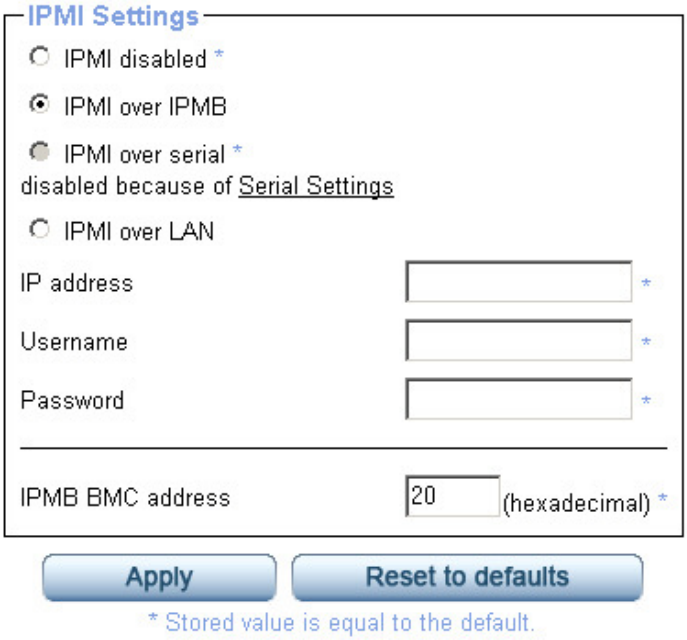


Figure 85 IPMI Settings

IPMI Settings

Figure 85 shows the ARMC/3P IPMI settings panel. Its options will be explained below.

IPMI disabled

Disables IPMI on the ARMC/3P. This means that Status (for example sensor and temperature information) via IPMI and Event Log via IPMI are not available.

IPMI over IPMB

This connection type uses an IPMB cable connected from the 1x5pin IPMB connector on the ARMC/3P card to the 3/4pin IPMB/I2C connector on the motherboard. IPMI over IPMB does not need any passwords. This access mode allows only power on/off and reset function. Status and Event Log via IPMI are disabled.

IPMI over LAN

You can connect the IPMI over a LAN connection, too. The prerequisite for

Downloaded from www.Manualslib.com manuals search engine

this access type is a host system with IPMI V1.5 and a network adapter with a sideband connection to the BMC (mostly on board). In the IPMI Settings you have to enter the IP address of this host system, the user name of a valid IPMI account and password for this account. You can also access other IPMI systems if you enter their IP address.

Date/Time

This link refers to a page where the internal realtime clock of the ARMC/3P can be set up (see Figure 86). You have the possibility to adjust the clock manually or to use a NTP time server. Without a time server your time setting will not be persistent, so you have to adjust it again after the ARMC/3P loses power for more than a few minutes. To avoid this you can use a NTP time server which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Important: There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

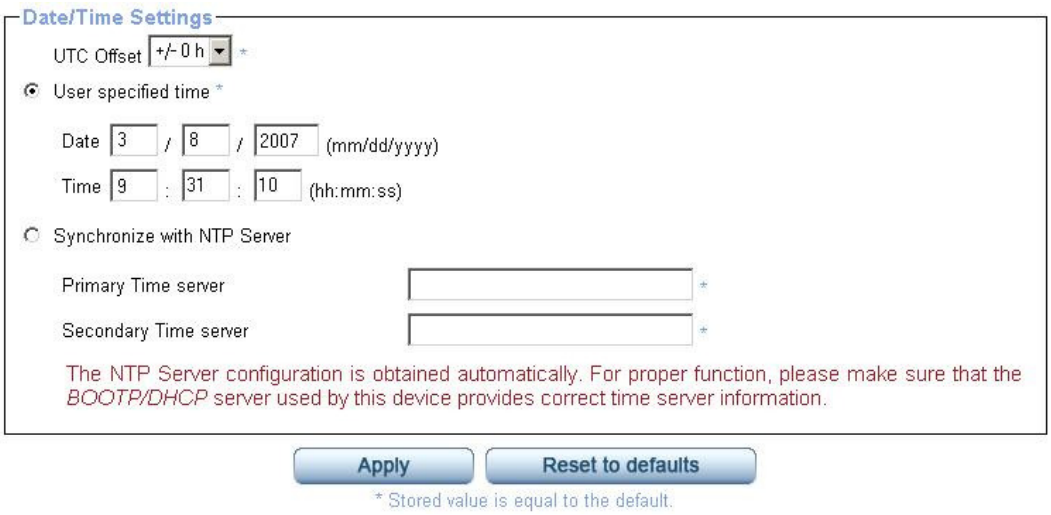

Date/Time Settings
UTC Offset +/- 0 h *
User specified time *
Date 3 / 8 / 2007 (mm/dd/yyyy)
Time 9 : 31 : 10 (hh:mm:ss)
Synchronize with NTP Server
Primary Time server *
Secondary Time server *
The NTP Server configuration is obtained automatically. For proper function, please make sure that the BOOTP/DHCP server used by this device provides correct time server information.
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 86 Date and Time

Authentication

With the ARMC/3P you have the possibility to use either a local authentication or keep the information in a central LDAP directory or in a RADIUS server. For LDAP or RADIUS you have to specify some information in the Authentication settings panel. For more information regarding the LDAP and RADIUS settings see below.

LDAP

User LDAP Server

Here you enter the name or IP address of the LDAP server containing all the

Downloaded from www.Manualslib.com manuals search engine

user entries. If you choose a name instead of an IP address you need to configure a DNS server in the network settings.

Base DN of User LDAP Server

Here you specify the distinguished name (DN) where the directory tree starts in the user LDAP server.

Type of external LDAP Server

With this option you set the type of the external LDAP server. This is necessary since some server types require special handling. Additionally, the default values for the LDAP scheme are set appropriately. You can choose between a Generic LDAP Server, a Novell Directory Service and a Microsoft Active Directory. If you have neither a Novell Directory Service nor a Microsoft Active Directory then choose a Generic LDAP Server and edit the LDAP scheme used (see below).

Name of login-name attribute

This is the name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected LDAP server type.

Name of user-entry object class

This is the object class that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type.

User search subfilter

Here you can refine the search for users that should be known to the ARMC/3P.

Active Directory Domain

This option represents the active directory domain that is configured in the Microsoft Active Directory server. This option is only valid if you have chosen a Microsoft Active Directory as the LDAP server type.

Downloaded from www.Manualslib.com manuals search engine

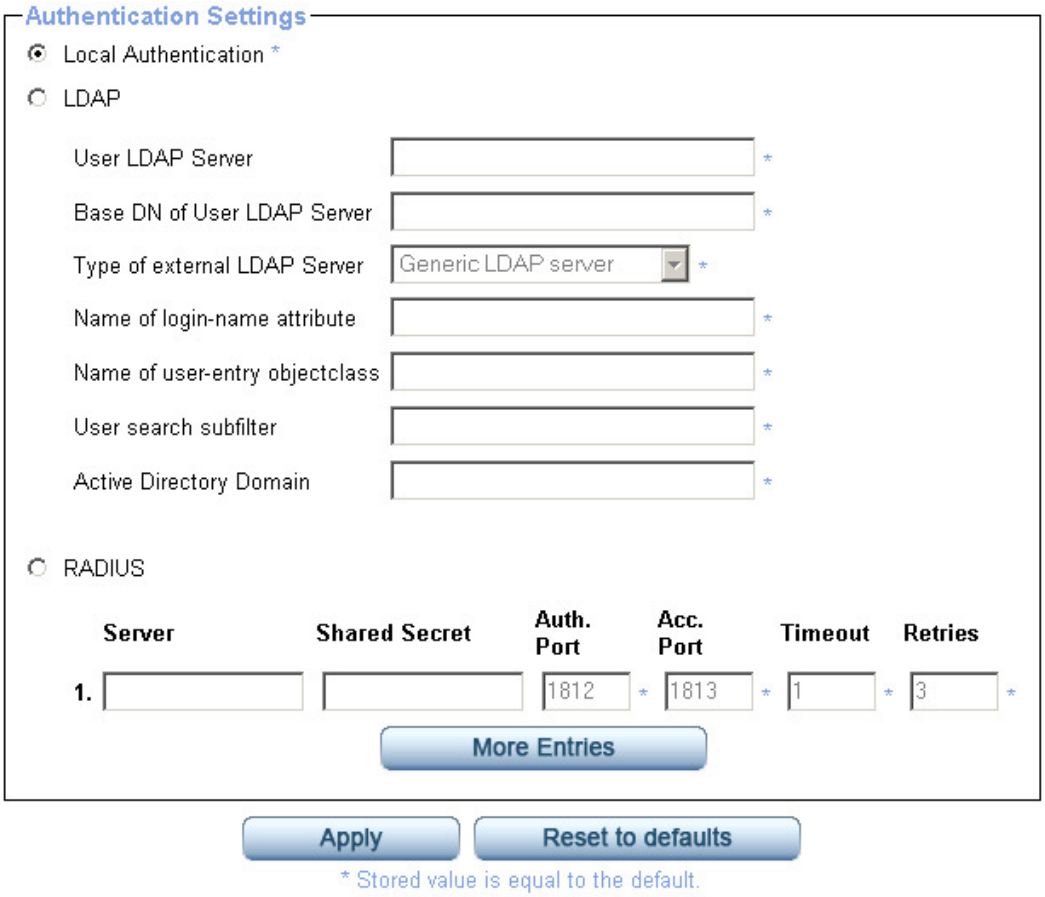


Figure 87 Authentication Settings

Remote Authentication Dial In User Service (RADIUS)

RADIUS is a protocol specified by the Internet Engineering Task Force (IETF) working group. There are two specifications that make up the RADIUS protocol suite: Authentication and Accounting. These specifications aim to centralize authentication, configuration, and accounting for dial-in services to an independent server.

The RADIUS protocol exists in several implementations such as freeRADIUS, openRADIUS or RADIUS on UNIX systems. The RADIUS protocol itself is well specified and tested. We can give a recommendation for all products listed above, especially for the freeRADIUS implementation.

Note: Currently, we do not support challenge/response. An Access Challenge response is seen and evaluated as an Access Reject.

To access a remote device using the RADIUS protocol you have to login, first. You are asked to specify your user name and password, then. The RADIUS server reads your input data (Authentication) and the ARMC/3P looks for your profile (Authorization). The profile defines (or limits) your actions and may differ depending onto your specific situation. If there is no such profile your access via RADIUS will be refused.

Downloaded from www.Manualslib.com manuals search engine

In terms of the remote activity mechanism the login via RADIUS works similar to the Remote Console. If there is no activity for half an hour your connection to the ARMC/3P will be interrupted and closed.

Server

Enter either the IP address or the hostname of the RADIUS Server to be connected. For the hostname DNS has to be configured and enabled.

Shared Secret

A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the ARMC/3P serves as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (message integrity). For the shared secret you can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z,a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation point (“!”) or an asterisk (“*”).

Authentication Port

The port the RADIUS server listens for authentication requests. The default value is #1812.

Accounting Port

The port the RADIUS server listens for accounting requests. The default value is #1813.

Timeout

Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the request. If the request job is not completed within this interval of time it is cancelled. The default value is 1 second.

Retries

Sets the number of retries if a request could not be completed. The default value is 3 times.

Event Log

Important events like a login failure or a firmware update are logged to a selection of logging destinations (see Figure 88). Each of those events belong to an event group which can be activated separately.

The common way to log events is to use the internal log list of the ARMC/3P. To show the log list click on the item **Event Log** from the section Maintenance. In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

Downloaded from www.Manualslib.com manuals search engine

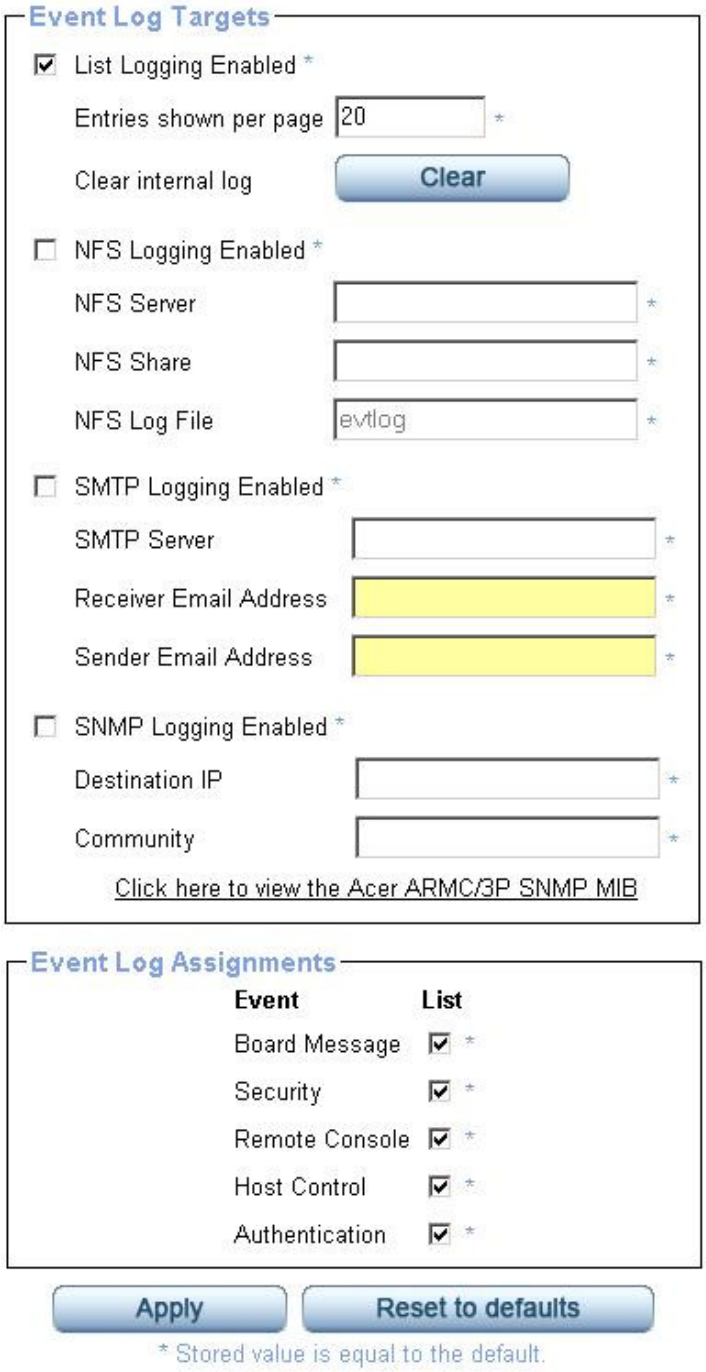


Figure 88 Event Log Settings

Event Log Targets

List logging enabled

To log events you may use the internal log list of the ARMC/3P. To show the log list click on **Event Log** on the Maintenance page. Since the ARMC/3P's system memory is used to save all the information, the maximum number of

Downloaded from www.Manualslib.com manuals search engine

possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one automatically.

Important: If the reset button on the HTML frontend is used to restart the ARMC/3P, all logging information is saved permanently and is available after the ARMC/3P has been started. If the ARMC/3P loses power or a hard reset is performed, all logging data will be lost. To avoid this use one of the log methods described below.

NFS Logging enabled

Define a NFS server where a directory or a static link has to be exported to, in order to write all logging data to a file that is located there. To write logging data from more than one ARMC/3P devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the **Apply** button, the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an error message.

Important: In contrast to the internal log file on the ARMC/3P, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

SMTP Logging enabled

With this option the ARMC/3P is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server that has to be reachable from the ARMC/3P device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the ARMC/3P sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have a own trap class that consists of several fields with detailed information about the occurred event. To receive these SNMP traps any SNMP trap listener may be used.

Event Log Assignments

You may choose which actions of the ARMC/3P will be saved in the log file. Tick the desired box(es) and click **Apply** to confirm your selection.

SNMP Settings

The following information is available via SNMP:

Downloaded from www.Manualslib.com manuals search engine

- Serial number
- Firmware version
- MAC address / IP address / Netmask / Gateway of LAN interface
- Server's power state

The following actions can be initiated via SNMP:

- Reset server
- Power on/off server
- Reset the ARMC/3P

The following events are reported by the ARMC/3P via SNMP:

- Login trial at the ARMC/3P failed.
- Login trial at the ARMC/3P succeeded.
- Denying access to a particular action.
- Server was reset.
- Server was powered on/off.

Figure 89 SNMP Settings

The SNMP settings panel as shown in Figure 89 is described below. It allows you to change SNMP related parameters.

Enable SNMP Agent

If this option is checked, the ARMC/3P will answer to SNMP requests.

Important: If a community is left blank, you cannot perform the according request. E.g. if you want to disable the possibility to reset the ARMC/3P via SNMP then do not set a write community.

Downloaded from www.Manualslib.com manuals search engine

Read Community

This is the SNMP community, which allows you to retrieve information via SNMP.

Write Community

This community allows you to set options and to reset the ARMC/3P or the host via SNMP, i.e. all that affects the host or the ARMC/3P.

System Location

Enter a description of the physical location of the host. The description will be used in reply to the SNMP request " sysLocation.0 ".

System Contact

Enter a contact person for the host. The value will be used in reply to the SNMP request " sysContact.0 ".

The ARMC/3P SNMP MIB

This link allows you to download the ARMC/3P SNMP MIB file. This file may be necessary for an SNMP client to communicate with the ARMC/3P.

Downloaded from www.Manualslib.com manuals search engine

Maintenance

Device Information

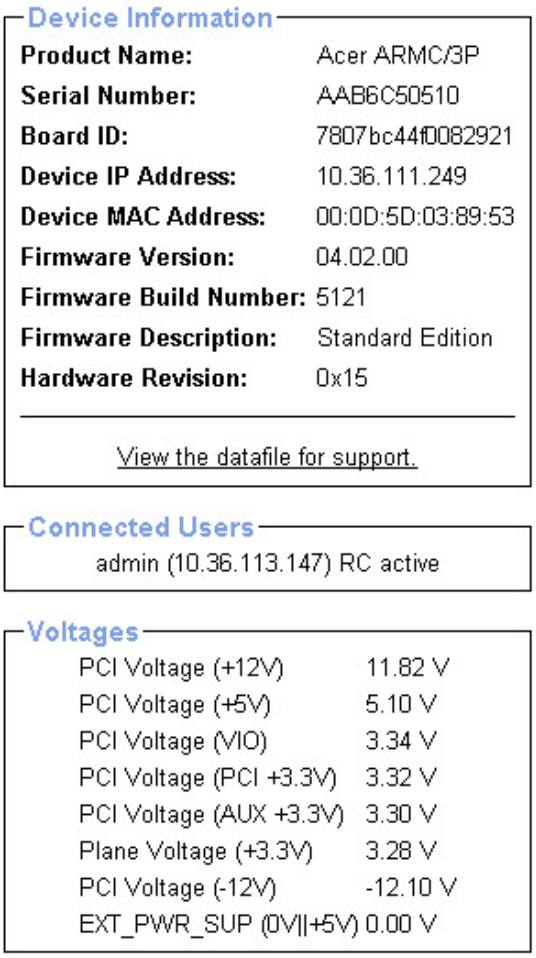

Device Information
Product Name: Acer ARMC/3P
Serial Number: AAB6C50510
Board ID: 7807bc44f0082921
Device IP Address: 10.36.111.249
Device MAC Address: 00:0D:5D:03:89:53
Firmware Version: 04.02.00
Firmware Build Number: 5121
Firmware Description: Standard Edition
Hardware Revision: 0x15
View the datafile for support.
Connected Users
admin (10.36.113.147) RC active
Voltages
PCI Voltage (+12V) 11.82 V
PCI Voltage (+5V) 5.10 V
PCI Voltage (VIO) 3.34 V
PCI Voltage (PCI +3.3V) 3.32 V
PCI Voltage (AUX +3.3V) 3.30 V
Plane Voltage (+3.3V) 3.28 V
PCI Voltage (-12V) -12.10 V
EXT_PWR_SUP (0V||+5V) 0.00 V

Figure 90 Device Information

This section contains a summary with various information about this ARMC/3P and its current firmware and allows you to reset the card. You may have a look at Figure 90 for an example.

The Data file for support allows you to download the ARMC/3P data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

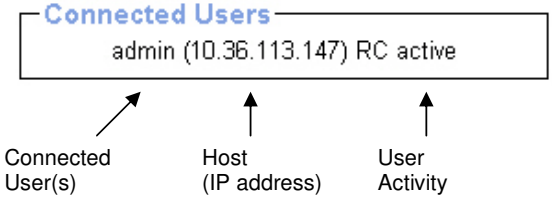


Figure 91 Connected Users

Downloaded from www.Manualslib.com manuals search engine

Figure 91 displays the ARMC/3P activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. “RC” indicates that the Remote Console is open. If the Remote Console is opened in “exclusive mode” the term “(exclusive)” is added. For more information about this option see Chapter 4: Remote Console Control Bar. To display the user activity the last column is used. It contains either the term “active” for an active user or the according idle time for an inactive user.

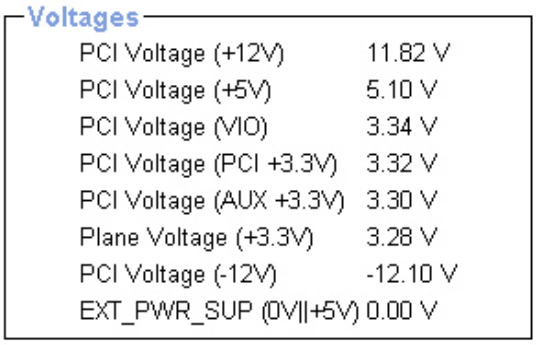

Voltages
PCI Voltage (+12V) 11.82 V
PCI Voltage (+5V) 5.10 V
PCI Voltage (VIO) 3.34 V
PCI Voltage (PCI +3.3V) 3.32 V
PCI Voltage (AUX +3.3V) 3.30 V
Plane Voltage (+3.3V) 3.28 V
PCI Voltage (-12V) -12.10 V
EXT_PWR_SUP (0V||+5V) 0.00 V

Figure 92 Voltages Overview

Figure 92 shows an overview of the different occuring Voltages of the ARMC/3P and the host system.

EXT_PWR_SUP (0V||+5V)
Shows only a voltage when the optional external power supply will be used.

Plane Voltage (+3.3V)
Shows the current voltage of the KIM G4.

PCI Voltages
Display the voltages for the PCI cards which are connected with the PCI Bus. A missing voltage could be a hint for a defective power supply.

Language

The ARMC/3P offers the choice between different languages for displaying the data in the front-end, like that shown in Figure 93.

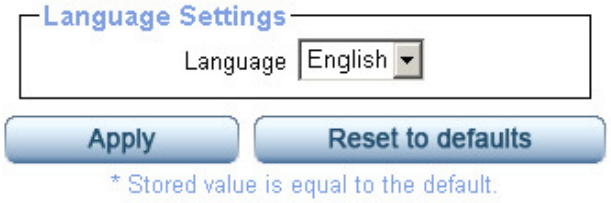


Figure 93 Language Settings

Downloaded from www.Manualslib.com manuals search engine

Event Log

Event Log

[Prev][Next]

Date	Event	Description
01/01/1970 01:18:42	Remote Console	Connection to client 10.36.113.147 established.
01/01/1970 01:17:59	Authentication	User 'admin' logged in from IP address 10.36.113.147
01/01/1970 00:00:42	Board Message	Device successfully started.
01/01/1970 00:00:41	Board Message	Device successfully started.
01/01/1970 00:00:41	Board Message	Device successfully started.
01/01/1970 00:12:34	Authentication	User 'admin' logged in from IP address 10.36.112.141
01/01/1970 00:12:32	Authentication	User 'admin' logged in from IP address 10.36.113.147
01/01/1970 00:03:18	Remote Console	Connection to client 10.36.111.234 closed.
01/01/1970 00:02:53	Remote Console	Connection to client 10.36.111.234 established.
01/01/1970 00:02:02	Authentication	User 'admin' logged in from IP address 10.36.111.234
01/01/1970 00:00:40	Board Message	Device successfully started.
01/01/1970 00:00:40	Board Message	Device successfully started.
01/01/1970 00:01:16	Board Message	Device successfully started.
01/01/1970 00:00:41	Board Message	Device successfully started.
01/01/1970 00:02:26	Authentication	User 'admin' logged in from IP address 10.36.111.51
01/01/1970 00:01:09	Remote Console	Connection to client 10.36.113.147 established.
01/01/1970 00:00:59	Authentication	User 'admin' logged in from IP address 10.36.113.147
01/01/1970 00:00:54	Authentication	User 'admin' failed to log in from IP address 10.36.113.147
01/01/1970 00:00:54	Authentication	User 'admin' failed to log in from IP address 0.0.0.0
01/01/1970 00:00:40	Board Message	Device successfully started.

[Prev][Next]

Figure 94 Event Log List

Figure 94 displays the Event Log list. It includes the events that are kept by the ARMC/3P extended by the event date, a short event description and an IP address the request was sent from. You may use the text buttons **Prev** and **Next** to browse within the data. The **Prev** button displays the previous page with newer log information whereas the **Next** button switches to the following page with older log information.

Update Firmware

Figure 95 Update Firmware Dialog

Downloaded from www.Manualslib.com manuals search engine

The ARMC/3P is a complete standalone computer. The software it runs is called the firmware. The firmware of the ARMC/3P can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email. If the firmware file is a compressed file with suffix `.zip` you have to unzip it before you can proceed. In order to extract the archive you may use WinZip from `http://www.winzip.com/` (for Windows OS) or a tool named unzip that might be already provided in your OS (UNIX, Linux, OS X).

Before you can start updating the firmware of your ARMC/3P the new and uncompressed firmware file has to be accessible on the system that you use for connecting to the ARMC/3P.

Updating the firmware is a three-stage process:

- First, the new firmware file is uploaded onto the ARMC/3P. In order to do that you need to select the file on your local system using the **Browse** button of the Upload Firmware panel (see Figure 95). Then, click **Upload** to transfer the previously selected file from your local file system onto the ARMC/3P. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted and the current firmware is kept as is.
- Second, if everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the **Update** button will store the new version and substitute the old one completely.

Important: This process is not reversible and might take some minutes. Make sure the ARMC/3P's power supply will not be interrupted during the update process, because this may cause an unusable device.

- Third, after the firmware has been stored, the ARMC/3P will reset automatically. After about one minute you will be redirected to the Login page and requested to login once again.

Important: The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the ARMC/3P's power supply will not be interrupted!

Unit Reset

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the ARMC/3P itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole

Downloaded from www.Manualslib.com manuals search engine

process will take about half a minute. Resetting subdevices (e.g. video engine) will take some seconds only and does not result in closing connections.

To reset a certain ARMC/3P functionality click on the **Reset** button as displayed in Figure 96.

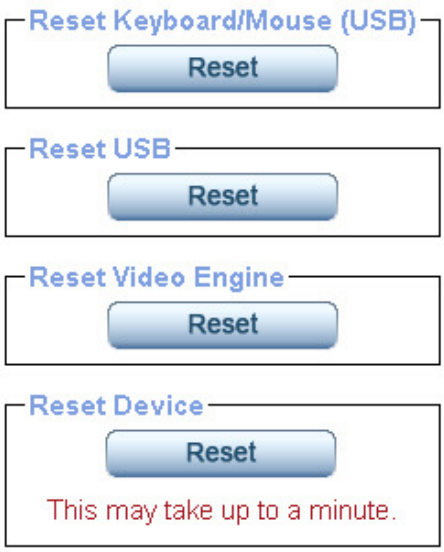


Figure 96 Unit Reset

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Appendix A: Specifications

Sizes and Weights

Table 11 ARMC/3P Specifications

Attribute	Value
Height	15mm (0.51‘’)
Width	167.64mm (6.6‘’)
Depth	64.41mmm (2.54’’)
Weight	112g (0.25lb)
Power Consumption	Up to 1A

Environment

Temperature

Table 12 Temperature

Attribute	Value
Operating	0℃ to 55℃ (32℉ to 131℉)
Storage	-18℃ to 70℃ (-0.4℉ to 158℉)

Humidity

Table 13 Humidity

Attribute	Value
Operating	10% to 90% (non-condensing)
Storage	5% to 95% (non-condensing)

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Appendix B: ARMC/3P Video Modes

Table 14 lists the video modes the ARMC/3P supports. Please do not use any other custom video settings besides these. If done so, the ARMC/3P may not be able to detect them.

Table 14 ARMC/3P Video Modes

Resolution (x,y)	Refresh Rates (Hz)
640x340	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
848x480	60, 70
960x600	60, 75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60, 85
1280x1024	60, 75, 85
1600x1200	60, 65, 70, 75
2048x1536	85 (local port only)

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Appendix C: Key Codes

Table 15 shows the key codes used to define the key strokes or hotkeys for several functions. Please note that these key codes do not necessarily represent the key characters that are used on international keyboards. A key on a standard 104 key PC keyboard with a US English language mapping is named. The layout for this keyboard is shown in Figure 97. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on a similar position, no matter what language mapping you are using. Some of the keys also have aliases. This means that a key can be named by two different key codes.

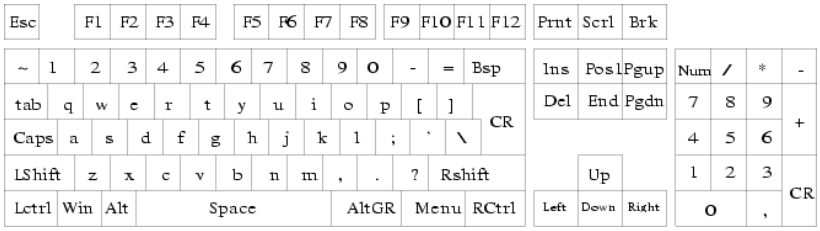

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prnt Scrl Brk
~ 1 2 3 4 5 6 7 8 9 0 - = Bsp Ins Pos1 Pgup Num / * -
tab q w e r t y u i o p [ ] CR Del End Pgdn 7 8 9 +
Caps a s d f g h j k l ; ` \ 4 5 6
LShift z x c v b n m , . ? Rshift Up 1 2 3 CR
Lctrl Win Alt Space AltGR Menu RCtrl Left Down Right 0 ,

Figure 97 English (US) keyboard Layout, used for the key codes

Table 15 Key Names

Key	Alias Key(s)
0 - 9	
A - Z	
~	TILDE
_	MINUS
=	EQUALS
;	
´	
<	LESS
,	
.	
/	SLASH
Backspace	
TAB	
[	
]	
ENTER	
CAPS LOCK	
\	BACK SLASH
LSHIFT	SHIFT
RCTRL	CTRL, STRG
RSHIFT	SHIFT
LCTRL	CTRL, STRG
LALT	ALT
SPACE	
ALT Gr	

Downloaded from www.Manualslib.com manuals search engine

Key	Alias Key(s)
ESCAPE	ESC
F1	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
PRINTSCREEN	
SCROLL LOCK	
BREAK	
INSERT	
HOME	POS 1
PAGE_UP	
PAGE_DOWN	
DELETE	DEL
END	
UP	
LEFT	
DOWN	
RIGHT	
NUM_LOCK	
NUMPAD0	
NUMPAD1	
NUMPAD2	
NUMPAD3	
NUMPAD4	
NUMPAD5	
NUMPAD6	
NUMPAD7	
NUMPAD8	
NUMPAD9	
NUMPADPLUS	NUMPAD_PLUS, +
NUMPAD /	/
NUMPADMUL	NUMPAD_MUL, *
NUMPADMINUS	NUMPAD_MINUS, -
NUMPADENTER	
WINDOWS	
MENU	

Downloaded from www.Manualslib.com manuals search engine

Appendix D: Pin Assignment

VGA HD-15

Figure 98 VGA HD-15

Table 16 VGA HD-15

PIN	Assignment	PIN	Assignment
1	Red	9	
2	Green	10	GND sync
3	Blue	11	
4		12	SDA, DDC…
5	GND	13	HSYNC
6	GND red	14	VSYNC
7	GND green	15	SCL, DDC
8	GND blue		

RJ45 Connetcor Ethernet

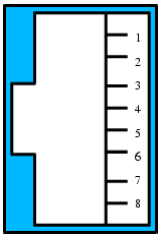


Figure 99 RJ45

Table 17 RJ45

PIN	Assignment	PIN	Assignment
1	TX +	5	Not connected
2	TX -	6	RX -
3	RX +	7	Not connected
4	Not connected	8	Not connected

IPMB/I2 Connector

Table 18 IPMB/I2C Connector

PIN	Assignment
1	IIC SCL (Clock)
2	Not connected
3	GND
4	IIC SDA (Data)
5	Not connected

Downloaded from www.Manualslib.com manuals search engine

Serial SUB-D9 Connector 1

Figure 100 Serial Connector

Table 19 Serial Connector 1

PIN	Assignment	PIN	Assignment
1	DCD	6	DSR
2	RX	7	RTS
3	TX	8	CTS
4	DTR	9	RI
5	GND		

Table 20 Serial Connetcor 2

PIN	Assignment	PIN	Assignment
1	Not connected	6	Not connected
2	RX	7	Not connected
3	TX	8	Not connected
4	Not connected	9	Not connected
5	GND		

PS/2 Connector

Table 21 PS/2 Connector

PIN	Assignment	PIN	Assignment
1	KBD_Data_Host	7	GND
2	KBD_CLK_Host	8	GND
3	Mouse_Data_Host	9	KBD_Data_DEV
4	Mouse_CLK_Host	10	KBD_CLK_Dev
5	+5V_Mouse_Host	11	Mouse_Dta_Dev
6	+5V_KBD_Host	12	Mouse_CLK_Dev

USB

Table 22 USB Connector

PIN	Assignment	PIN	Assignment
1	USB PWR	3	USB D+
2	USB D-	4	USB GND

Downloaded from www.Manualslib.com manuals search engine

Appendix E: Troubleshooting

1. The remote mouse does not work or is not synchronous.
   First, check the VGA connection. Both the ARMC/3P and the local monitor have to support the same video resolution.
   In some circumstances the mouse synchronization process could behave incorrectly, refer to the **Chapter 3:Mouse, Keyboard and Video configuration** for further explanation.

2. The video quality is bad or the picture is grainy.
   Enter the Remote Console and press the **Auto Adjust** button (see the Section called Remote Console Control Bar in Chapter 4) to adjust the ARMC/3P's video input parameters to the correct values.

3. Login on the ARMC/3P fails.
   Verify both your user login and your password. By default, the user "admin" has the password "password". Moreover, your web browser has to be configured to accept cookies.

4. The Remote Console window of the ARMC/3P does not open.
   A firewall may prevent the access to the Remote Console. The TCP ports #80 (for HTTP) and #443 (for both HTTPS and RFB) have to be open (the server providing the firewall has to accept incoming TCP connections on these ports).

5. Remote console is unable to connect and displays a timeout error.
   Have a look on your hardware. If there is a proxy server between the ARMC/3P and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the ARMC/3P and the client.
   Furthermore, check the settings of the ARMC/3P and choose a different server port used for RFB transfer. If you use a firewall then check the according port for accepting connections. You may restrict these connections for the IP addresses used by the ARMC/3P and your client.

6. No connection can be established to the ARMC/3P.
   Have a look on your hardware. Is the ARMC/3P attached to a power supply? Verify your network configuration (IP address, router). You may send a "ping" request to the ARMC/3P to find out whether the ARMC/3P is reachable via network.

7. Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.
   You have to define a so-called "Button Key". This can be done in the Remote Console settings (see the Section called Remote Console Control Bar in Chapter 5). Alternatively you can use the soft keyboard feature (see **Chapter 4: Soft Keyboard**).

8. The ARMC/3P web pages are not displayed correctly.
   Check your browser's cache settings. Make sure the cache settings are not set to something like "never check for newer pages". Otherwise the ARMC/3P pages may be loaded from your browser cache and not from the card.

Downloaded from www.Manualslib.com manuals search engine

9. Windows XP does not awake from standby mode.
   This is possibly a Windows XP problem. Try not to move the mouse pointer while XP switches into standby mode.

10. For SUN computers a USB keyboard does not work.
    The ARMC/3P emulates a USB keyboard. If you attach a USB keyboard to your host two keyboards are detected. It cannot be predicted which one of these comes first and you will be able to work with. SUN supports only one USB keyboard.

11. Cannot upload the signed certificate in MacOS X.
    If an “internal error” occurs while uploading the signed certificate either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to “plain text” and the checkbox “use for outgoing” is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).

12. Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore.
    Disable the setting “Automatically move mouse pointer to the default button of dialog boxes” in the mouse settings of your operating system.

13. The Remote Console does not open with Opera in Linux.
    Some versions of Opera do not grant enough permissions if the signature of the applet cannot be verified. To solve the problem, add the lines grant codeBase "nn.pp.rc.RemoteConsoleApplet" { permission java.lang.RuntimePermission "accessClassInPackage.sun.*"; to the java policy file of opera (e.g. /usr/share/opera/java/opera.policy).

14. I forgot my password. How can I reset the ARMC/3P to factory defaults?
    You may use the serial interface or the reset pins. For a detailed description see **Resetting the ARMC/3P to its Factory Settings in Chapter 3**.

15. The USB Keyboard does not work at the mainboard BIOS.
    Have a look on **Chapter 5: Virtual Media Options** and check if the **USB Mass Storage** is disabled. If it is still not working please check the USB Settings at the mainboard BIOS. Then check the Keyboard Mouse Settings under **Chapter 5: Keyboard/Mouse**. The Host Interface has to be **AUTO** or **USB.**

Downloaded from www.Manualslib.com manuals search engine

Appendix F: GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

Downloaded from www.Manualslib.com manuals search engine

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the

Downloaded from www.Manualslib.com manuals search engine

Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

Downloaded from www.Manualslib.com manuals search engine

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of

Downloaded from www.Manualslib.com manuals search engine

this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAWOR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTYWHOMAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

Downloaded from www.Manualslib.com manuals search engine

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FORAPARTICULAR PURPOSE. See theGNUGeneral Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type "show w". This is free software, and you are welcome to redistribute it under certain conditions; type "show c" for details.

The hypothetical commands “show w” and “show c” should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than “show w” and “show c”; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program “Gnomovision” (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Downloaded from www.Manualslib.com manuals search engine

Appendix G: The OpenLADAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine